

Informe de Transparencia en las Comunicaciones 2021

Índice

Reino Unido
Alemania
España
Mexico
Venezuela
Colombia
Ecuador
Perú
Brasil
Chile
Uruguay
Argentina

Introducción y alcance del Informe



En Telefónica estamos firmemente comprometidos con los derechos humanos de las personas y en especial con los derechos de privacidad y libertad de expresión. Trabajamos y velamos por su cumplimiento y además, promovemos una total transparencia en nuestras acciones a través de la publicación del Informe de Transparencia de las telecomunicaciones (7ª edición).

Tal y como ocurre en otras empresas de nuestro sector, en Telefónica recibimos **solicitudes de información** (ver definición en *glosario*) referidas a las comunicaciones de nuestros clientes o usuarios; solicitudes de bloqueo de acceso a ciertos sitios o contenidos o de filtrado de contenidos; o solicitudes con el objeto de suspender temporalmente el servicio en determinadas zonas o determinadas cuentas. Dichas solicitudes están cursadas por los cuerpos y fuerzas de seguridad del Estado, organismos gubernamentales y/o juzgados (en adelante: *autoridades competentes*, ver definición en glosario).

Por ello, la transparencia es un ejercicio imprescindible en un mundo en el que se comparten espacios de responsabilidad a la hora de preservar y garantizar los derechos de las personas. Por eso, en Telefónica hemos desarrollado Centros de Transparencia, tanto a nivel global como en los países donde operamos, donde nuestros grupos de interés pueden encontrar toda la información relevante de una manera sencilla, digital y comprensible respecto a la Privacidad, la Seguridad y la Libertad de Expresión.

En este ejercicio de transparencia, que se corresponde al periodo del 1 de enero de 2021 al 31 de diciembre de 2021, nuestro informe muestra:

i. nuestra debida diligencia en los derechos humanos;

ii. nuestra gobernanza en derechos humanos y, específicamente, en la privacidad y libertad de expresión;

iii. los compromisos, políticas y procesos que seguimos cuando respondemos a las solicitudes de las *autoridades competentes*;

iv. la información sobre el contexto legal que da potestad legal a las autoridades para hacer este tipo de solicitudes;

v. las autoridades que tienen potestad según la legislación local para cada uno de los indicadores que reportamos;

vi. el número total de solicitudes que recibimos durante el último año en cada uno de nuestros países de operación, a menos que se nos prohíba hacerlo o que un gobierno u otra entidad pública ya revele dicha información;

vii. y además, y cuando técnicamente es posible, reportamos el número de solicitudes que rechazamos, los accesos que son afectados por cada indicador y las url´s y/o IPs afectadas en el caso de bloqueo y restricción de contenidos.

1. El marco legal específico de cada país señala también limitaciones de cara a facilitar la información sobre los requerimientos que Telefónica recibe, por lo que en el informe se señalan ese tipo de limitaciones a la información que se aporta. Cuando no aportamos datos, explicamos por qué no los aportamos.

Nuestra debida diligencia en Derechos Humanos

Desde 2006, los derechos humanos forman parte integral de nuestros Principios de Negocio Responsable.

Los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas nos han servido de guía fundamental para fomentar la garantía y el respeto del derecho de las personas y, específicamente, en lo referente a la privacidad y libertad de expresión.

Nuestro enfoque de Derechos Humanos

* IA: Inteligencia Artificial

De acuerdo con nuestra Política Global de Derechos Humanos, contamos con una **debida diligencia** para identificar, prevenir, mitigar y remediar los impactos (potenciales y reales) de nuestro negocio en los derechos humanos. El punto de partida de la gestión de nuestra debida diligencia son las Evaluaciones de impacto globales, que se llevan a cabo cada tres/cuatro años a nivel global con la ayuda de expertos externos en derechos humanos y en estrecha consulta con nuestros grupos de interés. El objetivo de estas evaluaciones de impacto es averiguar cómo nuestras actividades/relaciones comerciales y productos/servicios impactan en los derechos humanos existentes y, sobre esta base, identificar los asuntos de derechos humanos más relevantes para nuestra actividad empresarial (ver gráfica asuntos de derechos humanos analizados en evaluaciones en impacto).

Por otro lado, basándonos en las evaluaciones globales y en los asuntos materiales identificados en ellas, realizamos análisis más detallados:

- Evaluaciones de riesgo anuales en todos nuestros mercados.
- Evaluaciones de impacto local, en aquellos casos en los que se considera relevante tener una visión más precisa de la situación nacional para identificar los riesgos en un contexto concreto.
- Evaluaciones de impacto temáticas, cuando necesitamos tener una visión más acotada de un asunto porque hemos detectado un riesgo o preocupación especial.

Contamos con un mecanismo de reclamación y remedio, nuestro Canal de consultas y denuncias, que permite a los grupos de interés, de forma confidencial y anónima, plantear quejas o consultas (en varios idiomas) sobre cualquier aspecto relacionado con los Principios de Negocio Responsable, explícitamente también sobre derechos humanos en general y privacidad y/o libertad de expresión en particular. El funcionamiento y gestión de dicho Canal se describe en el Reglamento sobre la gestión del Canal de Principios de Negocio Responsable y en la Política de gestión del Canal de Denuncias disponibles públicamente, y que garantizan el adecuado funcionamiento del Canal.



Nuestra gobernanza

Tenemos establecido un modelo de gestión de responsabilidades claras en la protección de los derechos humanos en general y en privacidad y libertad de expresión en particular.

Nuestras actividades en materia de derechos humanos, que incluyen asuntos relacionados con la privacidad y la libertad de expresión, se definen e implementan a través del **Plan de Negocio Responsable.** Aquí se establece la estrategia y los objetivos de sostenibilidad de la empresa, y es **aprobado y supervisado por el Consejo de Administración y la Comisión de Sostenibilidad y Calidad** (una de las Comisiones permanentes). Además, contamos con la **Oficina de Negocio Responsable** cuya finalidad es definir y monitorear el Plan de Negocio Responsable.

Este modelo de gobernanza, encabezado por el Consejo de Administración tiene como objetivo garantizar que nuestro compromiso con los derechos humanos se incorpore a todas las actividades y niveles de la empresa.

Gobernanza de Derechos Humanos: Privacidad y Libertad de Expresión

Consejo de Administración

Aprueba el Plan de Negocio Responsable (que incluye objetivos/medidas en relación con los derechos humanos/privacidad/libertad de expresión).

Comité Ejecutivo

Supervisa y ejecuta el Plan de Negocio Responsable.

Comisión de Sostenibilidad y Calidad (Comisión permanente del Consejo)

Supervisa la implementación del Plan de Negocio Responsable (que incluye objetivos/medidas en relación con derechos humanos/privacidad/libertad de expresión) a través de un reporte mensual.

Comisión de Auditoría y Control (Comisión permanente del Consejo)

Supervisa, entre otras cosas, cuestiones específicas relacionadas con la privacidad y la libertad de expresión mediante la presentación peródica del programa de cumplimiento en materia de privacidad.

Secretario del Consejo y Asuntos Regulatorios

Forma parte de Consejo de Administración y del Comité Ejecutivo y es responsable, entre otras cosas, de promover la privacidad/libertad de expresión con los grupos de interés externos relevantes en la materia.

Director de Sostenibilidad y Asuntos Corporativos

Forma parte del Comité Ejecutivo y es responsable de impulsar y supervisar diferentes iniciativas para promover respeto de los derechos humanos/privacidad/libertad de expresión.

Oficina de Negocio Responsable

La Oficina de Negocio Responsable (liderada por la Dirección de Ética Corporativa y Sostenibilidad) reúne a todos los directores de departamento relevantes en la Compañía para definir y monitorear el Plan de Negocio Responsable.

Compliance/Data Protection Officer

Es la función responsable dentro del Grupo de la coordinación de las inicativas relacionadas con la función de Delegado de Protección de Datos (art. 36 del Reglamento europeo de Protección de Datos).

Convoca y lidera

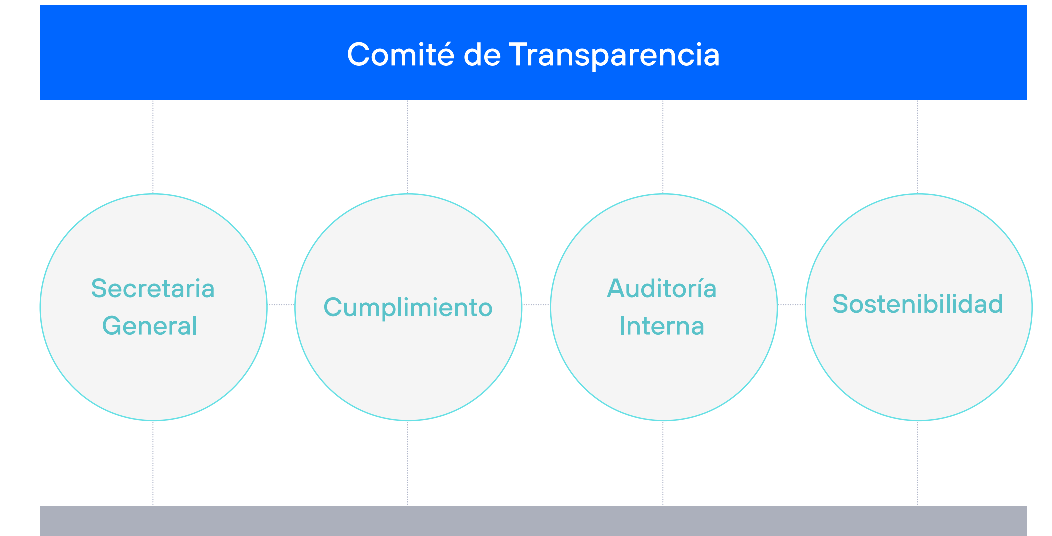
El ***Data Protection Officer* (DPO)** es el responsable dentro del Grupo de la coordinación de las iniciativas de protección de datos personales y reporta directamente al Consejo de Administración a través de la Comisión de Auditoría y Control (Comisión permanente del Consejo). El DPO coordina el *Steering Committee* en el que participan todas las áreas corporativas relevantes para asuntos específicos relacionados con la privacidad y la libertad de expresión. Como miembro de la Oficina de Negocio Responsable, el DPO también reporta regularmente a dicha Oficina las cuestiones relacionadas con su función.

Además, el **Secretario General y Asuntos Regulatorios** forma parte del Consejo de Administración y es responsable, entre otras cosas, de promover la privacidad y la libertad de expresión con los grupos de interés externos relevantes en la materia. En esta función, también dirigió la publicación y difusión del Pacto Digital en 2020, en el que se aboga por la cooperación entre los gobiernos, las empresas y la sociedad civil para definir un *New Digital Deal*' que adapte el entorno normativo actual a la era digital, prestando especial atención a las cuestiones de la privacidad y la libertad de expresión.

Por otro lado, en materia de gobernanza y gestión de este Informe, en el cual se recogen los requerimientos de las *autoridades competentes* y su relación con los derechos de privacidad y libertad de expresión, contamos con el **Comité de Transparencia** integrado por los responsables de las áreas globales de **Secretaría General, Cumplimiento, Auditoría Interna y Sostenibilidad**. Estos analizan los datos reportados de este informe, y pueden realizar las observaciones que consideren pertinentes, con carácter general o específicamente en relación con la información facilitada por las operadoras, con el objetivo de asegurar en todo momento la calidad de la información, como evidencia del cumplimiento de la normativa vigente y de la protección de los derechos fundamentales de las personas.

Aquellas solicitudes que por sus características y excepcionalidad así lo requieren, son analizadas por los máximos responsables de cada área responsable, mediante la adecuada ponderación de todos los intereses potencialmente comprometidos, incluidos los derechos humanos, libertades fundamentales u otros intereses que pudieran ser de aplicación y, si se diesen las circunstancias, por los órganos que dentro de cada compañía tengan entre sus funciones la evaluación y gestión de situaciones que pudieran eventualmente desembocar en una crisis.

En caso de crisis, se sigue un procedimiento establecido en el Sistema Global de Gestión de Crisis. Dentro de la taxonomia en este Sistema se mencionan de manera explícita



los incidentes críticos que pueden tener un impacto en la privacidad y en la libertad de expresión debido a:

- a) determinadas solicitudes de las autoridades.
- b) determinadas legislaciones.

El Sistema Global de Gestión de Crisis prevé que, en caso de una crisis relacionada con la cuestiones de libertad de expresión, el Presidente del Comité de Crisis puede convocar la denominada "Mesa Redonda de derechos humanos" (integrada por los departamentos pertinentes) para analizar la situación y diseñar y aplicar una estrategia de respuesta, informar al Comité Ejecutivo y realizar un análisis posterior con el fin de evitar un riesgo en el futuro.

Políticas y procesos de aplicación

Hemos impulsado y revisado diferentes políticas y procedimientos para asegurar la protección de los derechos de privacidad y libertad de expresión, el acceso a la información y la no-discriminación. A continuación, destacamos las políticas/procesos internos más importantes en materia de privacidad y libertad de expresión que se han adaptado a raíz de las ultimas evaluaciones de impacto.

Normativas

→ **Política Global de Derechos Humanos:**
Aprobada en el 2019. Esta política formaliza nuestro compromiso con los derechos humanos recogido, de forma general, en los Principios de Negocio Responsable de Telefónica, y de forma más específica en un conjunto de políticas y normas que velan por el respeto y aplicación de derechos humanos sociales, económicos y culturales internacionalmente reconocidos.

→ **Política de Privacidad:**
Actualizada en el 2018, forma parte de la estrategia de Telefónica para diseñar una nueva experiencia digital basada en la confianza (Confianza Digital).

Consciente de la importancia de merecer la confianza de nuestros clientes y/o usuarios y, con carácter general, de nuestros grupos de interés. Esta política les garantiza la legitimidad del tratamiento de sus datos por parte de Telefónica.

Establece unas normas de comportamiento común obligatorias para todas las entidades del Grupo, y un marco para una cultura de privacidad basada en los principios de licitud, transparencia, compromiso con los derechos de los interesados, seguridad y limitación del plazo de conservación.

Bajo el principio de transparencia garantizamos que a los interesados se les facilite de forma accesible e inteligible información sobre los datos personales que recogemos (tales como, a título de ejemplo: nombre, apellidos, dirección, cuenta bancaria, preferencias personales etc..), cómo los recogemos, la finalidad (prestación del servicio, etc..).

→ **Reglamento de Modelo de Gobierno de Protección de Datos:**
Tiene por objetivo englobar los aspectos más importantes a tener en cuenta para una correcta gestión y protección de los datos de carácter personal.

Se establece un modelo organizativo y de relación donde el máximo responsable de la Función de Protección de Datos Personales es el Delegado de Protección de Datos (DPO), quien reporta directamente al Consejo de Administración de Telefónica, S.A. Además, se articula a través de una estructura de relacionamiento y gobierno:

- **Oficina DPO:** Encargada de la supervisión del cumplimiento de la normativa de protección de datos del Grupo Telefónica.
- **Comité de Seguimiento:** Cuenta con la representación de diferentes áreas de la Compañía (Seguridad, Secretaría General, Regulación, Tecnología, CDO, Cumplimiento, Ética y Sostenibilidad y Auditoría Interna). Se revisa el estado general de cumplimiento del modelo de gobierno.
- **Comités de Negocio:** La Oficina DPO mantiene a través de la función técnica de Protección de Datos, interacciones permanentes con otras áreas, a través de los Responsables de Cumplimiento, al objeto de asegurar la máxima uniformidad en la aplicación de los procesos comunes, y/o la identificación y tratamiento de problemáticas específicas de privacidad en el ámbito de actividad de cada área.

→ **Reglamento ante Peticiones por parte de las *autoridades competentes*:**
En el 2019 se aprobó el Reglamento para reforzar el procedimiento ya existente desde 2016, con el objetivo de alinearlo con otras Políticas existentes y nuestros compromiso por el respeto a los derechos y libertades fundamentales. Define los principios y directrices mínimas que deben ser contemplados en los procedimientos internos propios de cada una de las compañías del Grupo/Unidades de Negocio/OB para cumplir con su deber de colaboración con las *autoridades competentes* de acuerdo con cada legislación nacional y con los derechos fundamentales de los interesados en este tipo de procedimientos.

Los principios que rigen el proceso son Confidencialidad, Exhaustividad, Fundamentación, Proporcionalidad, Neutralidad Política, Respuesta Diligente y Seguridad.

Nuestro compromiso es asegurar la participación en el proceso de áreas legales o áreas similares con competencias legales en la recepción de las solicitudes. Contamos con interlocutores fijos como ventanilla única en nuestra relación con las *autoridades competentes*, de manera que rechazamos cualquier solicitud que no viene por este conducto reglamentario.

→ **Política Global de Seguridad:**
Actualizada en el 2021 e inspirada en los principios de 'honestidad y confianza'. Esta política se rige por los estándares y regulaciones nacionales e internacionales en la materia, y establece los principios rectores en materia de seguridad que resultan aplicables a todas las empresas que integran el Grupo Telefónica.

Las actividades de seguridad se rigen por los siguientes Principios:

- **Legalidad:** Necesario cumplimiento de las leyes y regulaciones, nacionales e internacionales, en materia de seguridad.
- **Eficiencia:** Se destaca el carácter anticipativo y preventivo sobre cualquier potencial riesgo y/o amenaza con el objetivo de adelantarse y prevenir cualquier potencial efecto dañino y/o mitigar los perjuicios que pudieran causarse.
- **Corresponsabilidad:** El deber de los usuarios de preservar la seguridad de los activos que Telefónica pone a su disposición.
- **Cooperación y Coordinación:** Para alcanzar los niveles de eficiencia se prioriza la cooperación y la coordinación entre todas las unidades de negocio y empleados.

Fruto de esta Política, se han actualizado varias normativas de desarrollo para el efectivo cumplimiento de la misma. (Reglamento Gestión de Incidentes y Emergencias; Reglamento Análisis de Riesgos de Seguridad; Reglamento Seguridad en Redes y Comunicaciones; Reglamento de Ciberseguridad; Reglamento Seguridad en la Cadena de Suministro y el Reglamento Gobierno de la Seguridad entre otras.)

→ **Política de Comunicación Responsable:**
Aprobada en octubre del 2018, tiene por objetivo establecer las pautas de actuación para Telefónica en torno a nuestros canales de comunicación y generación de contenidos. Se basa en los Principios de Legalidad, Integridad y Transparencia, Neutralidad y Protección de Menores.

En el principio de neutralidad nos comprometemos a evitar posicionarnos políticamente como Compañía y promovemos el derecho a la libertad de expresión, dentro de los marcos regulatorios a los que estamos sometidos. En nuestra comunicación hacia clientes y a través de la publicidad prohibimos ciertas conductas que van en contra de nuestros Principios de Negocio Responsable. Así, en nuestros mensajes y nuestros patrocinios no toleramos que se abuse de la buena fe del consumidor, que atenten contra la dignidad de las personas, que fomenten el consumo del alcohol, el tabaco, las drogas, los trastornos alimenticios o el terrorismo, que inciten al odio, a la violencia o a la discriminación, a la comisión de comportamientos ilegales y puedan abusar de la ingenuidad del menor.

→ **Principios de Inteligencia Artificial:**
Aprobados por el Comité Ejecutivo en octubre del 2018, nos comprometemos a diseñar, desarrollar y usar la Inteligencia Artificial con Integridad y Transparencia. Son principios que sitúan a las personas en el centro y garantizan el respeto de los derechos humanos en cualquier entorno y proceso en el que se use la Inteligencia: Hacen hincapié en la igualdad e imparcialidad, la transparencia, la claridad, la privacidad y la seguridad. Son normas que aplican en todos los mercados en los que operamos y se extienden a toda nuestra cadena de valor, a través de socios y proveedores.

Durante el 2021, hemos estado trabajando en la implementación de estos principios en todas nuestras operaciones. Con un triple enfoque

- **Modelo estratégico:** A través de estos principios, nos comprometemos a diseñar, desarrollar y usar la Inteligencia Artificial, 1) de forma justa y no discriminatoria, 2) de manera transparente y explicable, 3) con las personas como prioridad, 4) con privacidad y seguridad desde el diseño y 5) con proveedores y socios que se comprometan con estas u otras normas éticas similares en materia de Inteligencia Artificial.
- **Modelo Organizativo y de relación:** Estamos implementando una IA responsable a través de un modelo organizativo y de relación que define qué departamentos de la empresa se ven involucrados, cuáles son sus funciones y cómo se relacionan entre sí para alcanzar un uso responsable de la IA.

Promovemos un enfoque de autorresponsabilidad con un modelo de escalación a demanda.

Los jefes/desarrolladores de producto que compran, desarrollan o utilizan la Inteligencia Artificial, deben realizar una simple autoevaluación desde el diseño del producto/servicio que están desarrollando mediante un cuestionario online. Esta autoevaluación

trata explícitamente los posibles riesgos que puede haber para los derechos humanos relacionados con el uso de la Inteligencia Artificial. Esta autoevaluación se integra en un modelo de gobernanza de tres niveles apoyado por una comunidad de expertos más amplia (entre ellos, una única persona de contacto para las cuestiones relacionadas con la IA y la ética, un «IA Champion» responsable o RAI). Si un jefe/desarrollador de producto (nivel1) tiene dudas sobre un posible impacto adverso de un determinado producto o servicio una vez completada la autoevaluación, y esta duda no puede resolverse con la ayuda de un RAI, se le planteará estas dudas automáticamente a un grupo de expertos multidisciplinar de la Compañía (nivel 2), que junto con el jefe/ desarrollador de producto intentarán resolver el problema.

En caso de que sea un riesgo potencial para la reputación de la empresa, el asunto se elevará a la Oficina de Negocio Responsable, que reúne a todos los directores de departamentos relevantes a nivel global (nivel 3).

→ Modelo Operativo

El modelo operativo describe los procedimiento para implementar el enfoque de IA responsable en el día a día de la empresa. Integrada dentro de una visión más amplia de la responsabilidad por diseño, incluye una metodología llamada «IA responsable por diseño» inspirada en metodologías ya existentes en privacidad y la seguridad por diseño. El modelo operativo consiste, entre otras cosas, en:

> **Actividades de formación y concienciación:** Telefónica ha desarrollado unos cursos relacionados con la IA y la ética que son accesibles a todos los empleados a través de los portales corporativos habilitados.

> **El cuestionario de autoevaluación,** donde cada principio de la IA se pone en práctica a través de una serie de preguntas para responder y una serie de recomendaciones. El cuestionario está dentro de la iniciativa global «Diseño Responsable» del grupo Telefónica.

> **Un conjunto de herramientas técnicas** que ayudan a responder a las preguntas del cuestionario de evaluación.

→ **Control interno:**

Telefónica cuenta con un modelo robusto de control que deberá ser oportunamente adaptado en lo necesario en cumplimiento de los requerimientos que pueda marcar la normativa aplicable.

Iniciativas y procesos

→ **Formación en derechos humanos:**

A finales del 2019 empezamos a trabajar a nivel global la formación en derechos humanos. Como en los años anteriores, impartimos formaciones generales para todos los empleados a través del Curso de Principios de Negocio Responsable y Derechos Humanos y una más específica para los profesionales (de las áreas Jurídica, Cumplimiento y Delegados de Protección de datos, equipo de M&A, Asuntos Públicos, Relaciones Institucionales y Operaciones), cuyo trabajo tiene un impacto mayor en los derechos humanos.

→ **Riesgo básico de derechos humanos:**

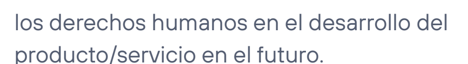
Los riesgos relacionados con impactos en derechos humanos se incluyen como un item específico en la gestión de riesgos del grupo Telefónica que debe ser evaluado anualmente por cada operación/país.

El objetivo es levantar cualquier riesgo de impacto, directo o indirecto, en las operaciones del Grupo Telefónica debido a posibles vulneraciones de derechos humanos, como consecuencia de la propia actividad de la Compañía o de la actividad que llevan a cabo nuestros proveedores u otras relaciones comerciales. Este análisis contempla cualquier cambio legislativo en los países o de actividad que pueda tener un impacto en los derechos humanos.

Este levantamiento de riesgos facilita definir las pautas de actuación necesarias en las operaciones directamente afectadas con el objetivo de mitigar y/o evitar estos riesgos y priorizar las actuaciones de Auditoría Interna, de cara a su planificación de actividades de supervisión de las estructuras de control interno.

→ **Derechos humanos por diseño:**

Evaluamos los posibles impactos en los derechos humanos de nuevos productos y servicios a través del enfoque 'derechos humanos desde el diseño', es decir, desde el inicio del diseño y/o comercialización de productos y servicios. Concretamente, los jefes de producto deben llevar a cabo una autoevaluación de nuevos productos y servicios a través de una herramienta en línea en la fase de diseño con el fin de identificar y abordar los posibles impactos en los derechos humanos ya en la fase de diseño. Los derechos humanos abordados en este cuestionario son, por ejemplo, privacidad, libertad de expresión, no- discriminación, Inteligencia Artificial, impacto en grupos vulnerables como los menores, etcétera. Si se identifican riesgos en materia de derechos humanos una vez finalizada la autoevaluación, el producto/ servicio en cuestión se somete a un análisis más detallado con la ayuda de expertos en derechos humanos de la empresa, a fin de abordar los posibles efectos adversos sobre



los derechos humanos en el desarrollo del producto/servicio en el futuro.

→ **Iniciativas de Transparencia:**
Uno de los retos y elementos clave en la privacidad es garantizar la transparencia. En Telefónica hemos apostado por llevarlo a la práctica incluyéndolo como uno de los Principios de la Política Global de Privacidad y desarrollando diferentes iniciativas que implementan este Principio, como son el Centro de Privacidad Global y los Centros de Privacidad o de Transparencia de las operadoras. Como parte del principio de transparencia, Telefónica pone a disposición de los clientes el acceso a los datos que generan durante el uso de nuestros productos y servicios, datos que son recogidos en el denominado 'Espacio de Datos Personales' de la 4ª plataforma y que resultan accesibles a través de diferentes canales como p. ej. el Centro de Transparencia en la *app* Mi Movistar.

En el año 2021 se concluyó el proceso de renovación total del Centro de Transparencia de Movistar en España disponible en su pagina web. https://www.movistar.es/Microsites/centro-transparencia/

Este centro ofrece a los clientes, el acceso a sus preferencias de privacidad y gestión de los datos recogidos en el espacio de Datos Personales.

En el Centro de Transparencia, a través de la sección Permisos de Privacidad, los clientes pueden gestionar las bases legitimadoras relativas al uso de sus datos para determinados propósitos. Y en la sección de Acceso y Descarga ofrecemos útiles visualizaciones de diferentes tipos de datos, con una experiencia amigable y respetando los criterios de privacidad, con la opción de descargar un documento con mayor nivel de detalle.

La experiencia del Centro de Transparencia se ha diseñado para dar confianza a los usuarios, con un lenguaje claro, y explicando el propósito para el cual se tratan sus datos y su naturaleza dentro de Telefónica.

Con el Centro de Transparencia se dan un paso más allá para cumplir nuestra promesa de empoderar a nuestros clientes con funciones de control y transparencia sobre sus datos, siempre de acuerdo con la normativa aplicable desde el punto de vista de la privacidad. Por ejemplo, en Europa este tratamiento estará plenamente alineado con el Reglamento Europeo de Protección de Datos.

→ **Aplicación efectiva de las políticas y procesos:**
De acuerdo con nuestra Política de Elaboración y Organización del Marco normativo, corresponde a la dirección de Auditoría Interna la coordinación del Marco Normativo del Grupo Telefónica, a través de la supervisión del proceso de definición de las normas Internas; promoviendo, a su vez, acciones que favorezcan la actualización y comunicación de las mismas. Adicionalmente detecta las necesidades y oportunidades de mejora, modificación o actualización de las Normas Internas existentes, proponiendo líneas de actuación a los Responsables de las Normas Internas, y proporcionar apoyo y asesoramiento al Responsable de la Norma Interna en relación con su redacción e implantación.

La observancia y cumplimiento de la normativa (p. ej. las políticas de privacidad, seguridad etc. mencionadas) son objeto de revisión y supervisión por parte de los responsables de las Normas Internas que lideran la propuesta, creación, difusión e implantación de la Norma interna y realizan su seguimiento, evaluación y actualización, quien está facultada para realizar las supervisiones muestrales de los controles siempre que lo considere conveniente.

Adicionalmente, y en línea con lo establecidopor la Comisión Nacional del Mercado de Valores (CNMV) y lo previsto en el art. 22 del Reglamento del Consejo de Administración de Telefónica, S.A., entre las competencias de la Comisión de Auditoría y Control del Consejo, se encuentra la de "supervisar la eficacia del control interno de la Sociedad, la auditoría interna y los sistemas de gestión de riesgos".

RDR (Ranking Digital Rights) y GNI (Global Network Initiative)



Además, quedamos primeros entre todas las empresas de telecomunicaciones del *Ranking Digital Rights* que se publicó en febrero 2021, y que evalúa los compromisos, políticas y prácticas de las empresas que afectan a la libertad de expresión y a la privacidad de los clientes, incluidos los mecanismos de gobernanza y supervisión.

Como miembros del Global Network Initiative (GNI), en 2021, hemos participado en diferentes iniciativas relacionadas con el impacto del COVID-19 sobre la privacidad y la libertad de expresión. Además, pasamos con éxito el proceso de evaluación independiente del GNI. La evaluación positiva del GNI se basó en un informe de un asesor externo independiente (Deloitte) que examinó las políticas, los procesos, y el modelo de gobernanza de Telefónica para salvaguardar la libertad de expresión y la privacidad de sus clientes.

Indicadores de este Informe

En los apartados siguientes reportamos el número de solicitudes que recibimos por parte de las autoridades nacionales competentes en los países donde operamos.

Cualquier solicitud que se pueda recibir por parte de una autoridad competente nacional debe cumplir con los procesos judiciales y/o legales que corresponda a cada país. En Telefónica solo atendemos solicitudes que provengan de una autoridad nacional competente siguiendo nuestro Reglamento ante Peticiones por parte de las *autoridades competentes*. En Telefónica **no atendemos solicitudes privadas,** solo se tramitan las solicitudes que provienen de autoridades determinadas por ley. Dicho esto y como única excepción, en la lucha proactiva contra los contenidos de imágenes de abusos sexuales a menores de edad en la Red, Telefónica procede al bloqueo de estos materiales siguiendo las pautas y las listas proporcionadas por la Internet Watch Foundation.

Los indicadores que reportamos son:

Interceptaciones legales

Aquellas solicitudes que proceden de las *autoridades competentes* en el marco de investigaciones criminales, y en su caso, civiles, con el objetivo de interceptar comunicaciones o acceder a datos de tráfico en tiempo real.

Se incluye el desglose de Interceptaciones, siempre y cuando sea técnicamente y/o legalmente posible, por:

- **Altas:** Solicitudes de una nueva interceptación.
- **Prórrogas:** Solicitudes para prorrogar una interceptación ya existente.
- **Bajas:** Solicitudes para desconectar a una interceptación existente.

Metadatos asociados a las comunicaciones

Aquellas solicitudes procedentes de las *autoridades competentes* que tienen por objetivo obtener datos históricos referidos a:

- el nombre y dirección del usuario registrado (datos de abonado);
- los datos para identificar el origen y el destino de una comunicación (por ejemplo, números de teléfono, nombres de usuario para los servicios de Internet);
- la fecha, hora y duración de una comunicación;
- el tipo de comunicación;
- la identidad de los equipos de comunicación (incluyendo IMSI o IMEI);
- la localización del dispositivo del usuario.

Bloqueo y restricción de contenidos

Aquellas solicitudes de las *autoridades competentes* para bloquear el acceso a sitios web específicos o a un determinado contenido.
Se trata de solicitudes para bloquear el acceso a un sitio web o a un contenido, no una petición para eliminar el contenido del usuario. A título de ejemplo, las demandas de bloqueo se emiten porque los sitios web o determinados contenidos que publican son contrarios a las leyes locales (suelen estar relacionados con material de abuso sexual infantil, los juegos de azar online, violación de derechos de autor, difamación, venta ilegal de medicamentos, armas, marca comercial, etc.).
Se incluye el desglose el desglose por tipo de bloqueo, cuando las herramientas y la legislación lo permiten.

Suspensiones geográficas o temporales de servicio

Aquellas solicitudes requerimiento de las *autoridades competentes* para limitar temporal y/o geográficamente la prestación de un servicio. Estos requerimientos suelen estar relacionados con situaciones de fuerza o causa mayor como catástrofes naturales, actos de terrorismo, etc. También se contabilizan las restricciones de acceso individuales.

También se contabilizan las restricciones de acceso individuales.

Además, para cada indicador reportamos también los siguientes subindicadores:

Solicitudes rechazadas o atendidas parcialmente

Número de veces que hemos rechazado una solicitud o que solo hemos proporcionado información parcial o ninguna información en respuesta a una solicitud por alguna de las siguientes razones:

- **Por no ajustarse a la legislación local para ese tipo de requerimiento.**
- **Por no contener todos los elementos necesarios que posibilita la ejecución (firmas necesarias, autoridad competente, descripción técnica del requerimientos etc...)**
- **Porque técnicamente es imposible ejecutar el requerimiento.**

Accesos afectados

Número de accesos que se ven afectados por cada solicitud. Para bloqueo y restricción de contenidos contabilizamos Url's afectadas.

Pueden existir variaciones notables en los datos de cada uno de los indicadores respecto a años anteriores que suelen ser debidos por razones técnicas, metodológicas o legislativas.

Por otra parte, pueden existir variaciones respecto a años anteriores debido a solicitudes con potencial impacto en los derechos a la libertad de expresión y de privacidad; identificamos dichas solicitudes como major events.

Cabe destacar la situación de excepcionalidad en la que continúa Venezuela y los retos a los que nos enfrentamos para la verificación de nuestros procesos globales en el país. En esta situación, Telefónica debe priorizar el cumplimiento con la legislación vigente, el mantenimiento de la conectividad en el país y el bienestar de nuestros empleados.

Y por último, tras los eventos acontecidos desde que el mes de febrero 2022 diera comienzo el conflicto entre Rusia y Ucrania, son numerosas las medidas a nivel internacional que se han llevado a cabo; algunas de ellas con posible impacto en los derechos humanos en general y privacidad y libertad de expresión en particular. Aunque si bien es cierto, que dicho acontecimiento no se enmarca dentro el periodo de reporte que concierne este documento (enero 2021 – diciembre 2021) y tampoco tenemos presencia como operadora en dichas regiones, tenemos el compromiso y la responsabilidad de considerar posibles impactos que pudiera tener nuestra actividad en materia de derechos humanos en general, y privacidad y libertad de expresión en particular. Ello nos lleva a que esta crisis y sus consecuencias internacionales sean consideradas en los diferentes comités que se llevan a cabo en Telefónica con la finalidad de velar por el respeto por los derechos humanos, la privacidad y libertad de expresión en el caso de que fuera necesaria una intervención por parte del Grupo y se dará cuenta de ello en el informe del próximo año.

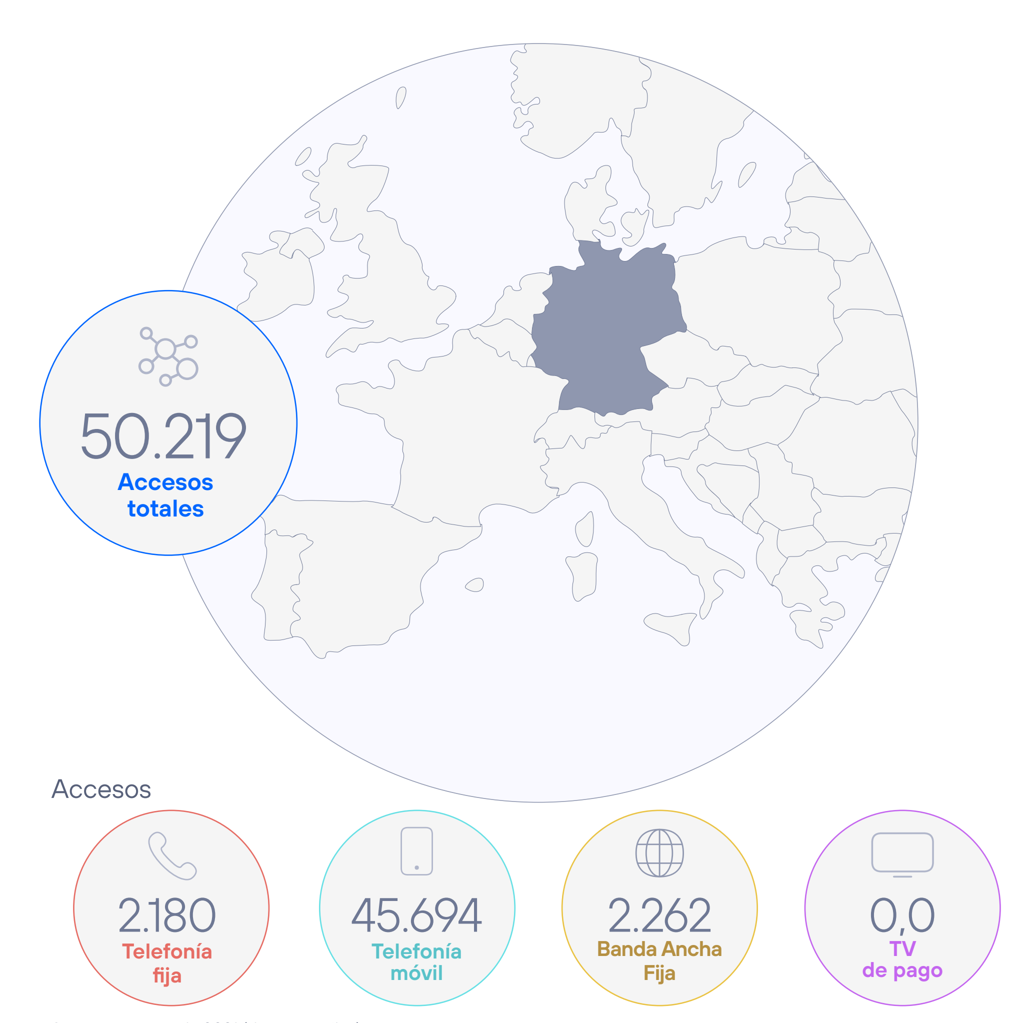
Informe por país



- → Alemania
- → Argentina
- → Brasil
- → Chile
- → Colombia
- → Ecuador
- → España
- → México
- → Perú
- → Reino Unido
- → Uruguay
- → Venezuela

Alemania

www.telefonica.de



Accesos a cierre de 2021 (datos en miles).

Telefónica cuenta con un largo historial en Alemania y opera bajo la marca comercial O2.

Telefónica Deutschland ofrece telefonía móvil de pre-pago y contrato a clientes residenciales y empresas, e innovadores servicios de datos a través de las tecnologías GPRS, UMTS y LTE. Como proveedor integrado de comunicación, también ofrece servicios de ADSL e internet de alta velocidad. Telefónica cuenta con un total de 50,2 millones de accesos en Alemania.

Los ingresos totales de Telefónica en Alemania se sitúan en 7.765 millones de euros y el OIBDA en 2.424 millones de euros.



Información a cierre de 2021

Interceptación legal

Contexto legal

→Ley de Telecomunicaciones, Sección 170 (*Telekommunikationsgesetz* - TKG).

→Código de Procedimiento Penal (StPO *The German Code of Criminal Procedure*).

→Ley articulo 10 G10, Sección 100, Artikel 10 Gesetz - G10.

→Ley de servicios de investigaciones aduaneras (ZFDG).

→Ley federal de la oficina de policía penal (BKAG).

→Leyes policiales de los estados federales (*Landespolizeigesetze*).

Autoridades Competentes

→Agencias y Cuerpos de Seguridad del Estado (*Law Enforcement Agencies*-LEAs) como autoridades policiales (nacional y federal) y servicios de inteligencia y aduanas (nacional y federal).

→Las medidas recogidas en la Sec. 100a del Código de Procedimiento Penal alemán (StPO) requieren una orden judicial previa. En caso de circunstancias extremas, el Ministerio Público podrá emitir una orden, que deberá ser confirmada por un Juzgado dentro de los tres días hábiles siguientes para que resulte eficaz.

Solicitudes*



* El volumen total incluye nuevas, prorrogas y cese de interceptaciones.

** En 2020, el aumento comparado con 2019, es debido a un cambio en el registro de requerimientos. Es decir, se ha hecho un registro por número de solicitudes y no por número de peticiones, lo que permite dar una información más granular (una petición puede contener varias solicitudes, ver glosario).

*** Este resultado se debe a que se insta a las Autoridades a su corrección

Metadatos asociados a las comunicaciones

Contexto legal

→Ley de Telecomunicaciones Aleman Sec. 9 and 12 TTDSG (Telecommunications and Telemedia Data Protection Act) and Sec 176 TKG.

→Código de Procedimiento Penal Sec. 100g (*Strafprozessordnung* – StPO).

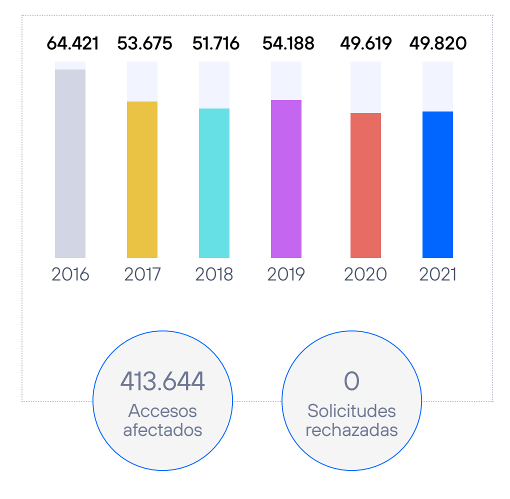
→Leyes policiales de los estados federales (*Landespolizeigesetze*).

Autoridades Competentes

→Agencias y Cuerpos de Seguridad del Estado (*Law Enforcement Agencies*-LEAs) como autoridades policiales (nacional y federal) y servicios de inteligencia y aduanas (nacional y federal).

→Las medidas recogidas en la Sec. 100a del Código de Procedimiento Penal alemán (StPO) requieren una orden judicial previa. En caso de circunstancias extremas, el Ministerio Público podrá emitir una orden, que deberá ser confirmada por el Juzgado dentro de los tres días hábiles siguientes para que resulte eficaz.

Solicitudes*



* Número de peticiones



Bloqueo y restricción de contenidos

Contexto legal
CUII "Clearingstelle Urheberrecht im Internet", acuerdo sectorial de proveedores de servicios de Internet (ISPs) y las industrias de derecho de autor (11/03/2021).

Autoridades Competentes
No aplica.

Solicitudes



*En 2021 se implementó el acuerdo sectorial, CUII, para efectuar bloqueos por causa de la piratería de contenidos.

Tipología: 27 propiedad intelectual y 1 por supervisión financiera.

Suspensiones geográficas o temporales de servicio

Contexto legal
CUII "Clearingstelle Urheberrecht im Internet", acuerdo sectorial de proveedores de servicios de Internet (ISPs) y las industrias de derecho de autor (11/03/2021).

Autoridades Competentes
No aplica.

Solicitudes





Argentina

www.telefonica.com.ar



Accesos a cierre de 2021 (datos en miles).

Telefónica está presente en Argentina desde la privatización de los servicios telefónicos en 1990. A lo largo de estos años, la compañía se ha convertido como un grupo líder de empresas especializado en telecomunicaciones integradas.

Tras haber sido la primera inversión significativa de capitales españoles, contribuyó en estos años al desarrollo de las comunicaciones mediante inversiones de infraestructuras y una amplia oferta de servicios de telefonía fija, móvil e Internet.

Telefónica en Argentina gestiona más de 21,7 millones de accesos a diciembre de 2021.

Respecto a las cifras financieras, los ingresos de Telefónica en Argentina alcanzaron 2.056 millones de euros y el OIBDA sumó 229 millones de euros.



Información a cierre de 2021

Interceptación legal

Contexto legal

→ Constitución Nacional Argentina, artículo 18.

→ Ley 19.798, Inviolabilidad de las comunicaciones, artículos 18 y 19.

→ Ley 27.078, Inviolabilidad de las comunicaciones, artículo 5.

Autoridades Competentes

→ Son los jueces los únicos autorizados a solicitar la intervención judicial sobre un acceso, y los Fiscales únicamente en caso de tratarse de un delito de Secuestro Extorsivo en curso, en cuyo supuesto podrán solicitar la intervención, debiendo ser ratificada por un juez en un plazo máximo de 24 horas. En cuanto al procedimiento, los juzgados solicitan la intervención a la denominada Dirección de Asistencia Judicial en Delitos Complejos (DAJDECO), organismo dependiente de la Corte Suprema de Justicia de la Nación, quienes luego formalizan y dan curso el pedido de intervención a las empresas prestatarias de servicios.

Solicitudes



Metadatos asociados a las comunicaciones

Contexto legal

→ Constitución Nacional Argentina, artículo 18.

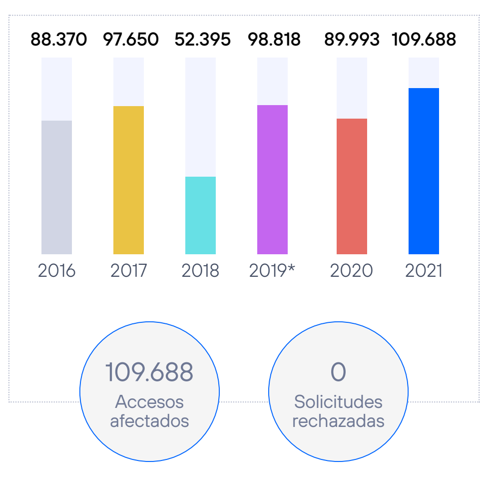
→ Ley 19.798, Inviolabilidad de las comunicaciones, artículos 18 y 19.

→ Ley 27.078, Inviolabilidad de las comunicaciones, artículo 5.

Autoridades Competentes

→ Jueces, Fiscales y los cuerpos y fuerzas de seguridad del Estado al que se le haya delegado la investigación.

Solicitudes



*En el 2019 se empezó a registrar los datos de Acceso a Metadatos, Bloqueo de contenidos y Suspensión del Servicio de manera separada y no agregada como en años anteriores por lo que la comparación interanual debe hacerse desde 2019 en adelante.

Bloqueo y restricción de contenidos

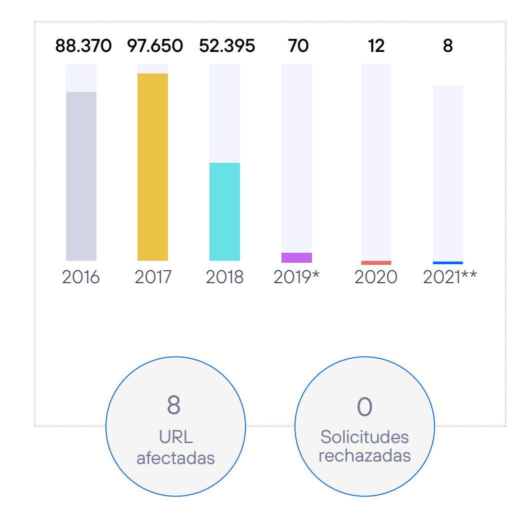
Contexto legal

→ Ley 27.078, Inviolabilidad de las comunicaciones, artículo 5.

Autoridades Competentes

→ Jueces, Fiscales y los cuerpos y fuerzas de seguridad del Estado al que se le haya delegado la investigación.

Solicitudes



*En el 2019 se empezó a registrar los datos de Acceso a Metadatos, Bloqueo de contenidos y Suspensión del Servicio de manera separada, y no agregada como en años anteriores, por lo que la comparación interanual debe hacerse desde 2019 en adelante.

** Se bloquearon, a pedido judicial, sitios con denuncias por phishing, juego online sin autorización, etc

Suspensiones geográficas o temporales de servicio

Contexto legal

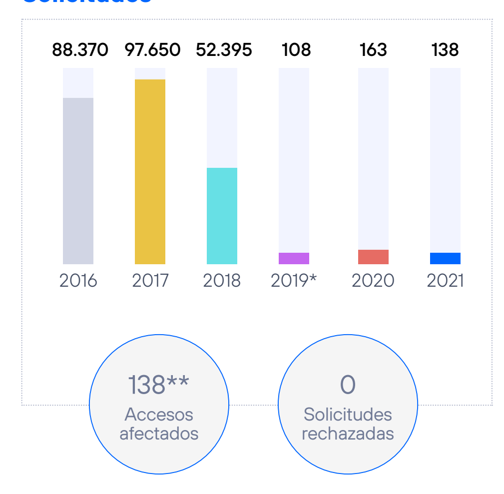
Si bien no existe una norma específica que lo regule, podría interpretarse que forma parte de lo establecido en el Art. 57 de la Ley 27.078, en cuanto dispone;

Neutralidad de red. Prohibiciones. Los prestadores de Servicios de TIC no podrán: Bloquear, interferir, discriminar, entorpecer, degradar o restringir la utilización, envío, recepción, ofrecimiento o acceso a cualquier contenido, aplicación, servicio o protocolo salvo orden judicial o expresa solicitud del usuario.

Autoridades Competentes

Al no haber una norma específica, el único órgano competente para dictar una medida de suspensión del servicio en una determinada zona es un juez con competencia federal.

Solicitudes



138** Accesos afectados

0 Solicitudes rechazadas

*En 2019 se empezó a registrar los datos de Acceso a Metadatos, Bloqueo de contenidos y Suspensión del Servicio de manera separada y no agregada como en años anteriores, por lo que la comparación interanual debe hacerse desde 2019 en adelante. Corresponden a solicitudes para restringir temporalmente el tráfico de datos móviles de determinados clientes.

**bloqueos individuales de datos.



Brasil

www.telefonica.com.br



Accesos

Telefonía fija	Telefonía móvil	Banda Ancha Fija	TV de pago
7.506	83.912	6.262	1.115

Accesos a cierre de 2021 (datos en miles).

Telefónica entró en el mercado brasileño en 1998, momento en el que se estaba produciendo la reestructuración y privatización de Telebrás.

Más adelante, en el año 2002, Telefónica y Portugal Telecom crean una Joint Venture para operar en el mercado móvil brasileño e inician sus operaciones comerciales con el nombre de Vivo en abril de 2003.

Durante el año 2015, se cerró la adquisición de GVT, lo que sitúa a Telefónica Brasil como el operador integrado líder del mercado brasileño.

Telefónica en Brasil gestiona más de 98,8 millones de accesos a diciembre de 2021.

Respecto a las cifras financieras, los ingresos de Telefónica en Brasil alcanzado los 6.910 millones de euros y el OIBDA, 3.138 millones de euros.



Información a cierre de 2021

Interceptación legal

Contexto legal

- Constitución de la República Federal de Brasil, artículo 5.
- Ley Nº 9.296, 24/07/1996.
- Nueva regulación: Resolución 73/1998, en los términos de resolución 738/2020 de 21/12/2020.

Autoridades Competentes

- De acuerdo con el artículo 3º de la Ley Federal brasileña n. 9.296/1996 (Ley de las Interceptaciones), solamente el Juez (de la esfera criminal) puede determinar las interceptaciones (telefónicas y telemáticas), a petición de la Fiscalía *(Ministério Público)* o Comisario de Policía *(Autoridade Policial)*.

Solicitudes



*El sistema de registro durante el periodo de reporte no disponía de los mecanismos para filtrar por peticiones rechazadas. Se está trabajando para disponer de este dato en los próximos informes.

Metadatos asociados a las comunicaciones

Contexto legal

- Ley Nº 9.296, 24/07/1996.
- Ley Nº 9.472, artículo 3, 16/07/1997.
- Ley Nº 12.683, artículo 17 B, 09/07/2012.
- Ley Nº 12.830, artículo 2, 20/07/2013.
- Ley Nº 12850, artículo 15, 20/08/2013.
- Ley Nº 12965, artículo 7, 10 y 19, 23/04/2014.
- Decreto Nº 8.771, artículo 1, 11/05/2016.
- Ley N.º 13344, artículo 11, 10/2016.
- Ley N.º 13812, artículo 10, 05/2019.
- Resolución n.º 73 del 25 del noviembre de 1998 / Reglamento de Servicio de Telecomunicaciones – Art. 65 – K.
- Resolución n.º 632 del del 7 de marzo de 2014 / Reglamento General de Derechos del Consumidor de Servicios de Telecomunicaciones – RGC – Art. 3º, V.

Autoridades Competentes

- Fiscalía, Comisarios de Policía y Jueces de cualquier esfera, como también Presidentes de las Comisiones Parlamentarias de Investigación: el nombre y dirección del usuario registrado (datos de abonado), así como la identidad de los equipos de comunicación (incluyendo IMSI o IMEI).
- Jueces de cualquier esfera: los datos para identificar el origen y el destino de una comunicación (por ejemplo, números de teléfono, nombres de usuario para los servicios de Internet), la fecha, hora y duración de una comunicación y la localización del dispositivo.

Solicitudes



*El sistema de registro durante el periodo de reporte no disponía de los mecanismos para filtrar por peticiones rechazadas. Se está trabajando para disponer de este dato en los próximos informes.

Bloqueo y restricción de contenidos

Contexto legal

Ley N° 12965, artículo 7 y 19, 23/04/2014.

Autoridades Competentes

Exclusivamente Jueces.

Solicitudes



* El sistema de registro durante el periodo de reporte no disponía de los mecanismos para filtrar por peticiones rechazadas. Se está trabajando para disponer de este dato en los próximos informes.

**Aclaración: Pasadas las medidas de bloqueos generales que afectaron a todos los clientes en potencial, las autoridades públicas empezaron a practicar bloqueos individuales en el ámbito de investigaciones criminales.

***En el 2019 se contabilizan solo bloqueo de URL's dejando las suspensiones del servicios de whatsapp en el indicador "Suspensión del Servicio".

****El incremento respecto al año 2019 se debe a una campaña por parte del Ministerio de Justicia de Brasil para combatir la Piratería (Operación 404).

Suspensiones geográficas o temporales de servicio

Contexto legal

Resolución n.° 73 del 25 del noviembre de 1998 / Reglamento de Servicio de Telecomunicaciones – Art. 65 – K.

Autoridades Competentes

Únicamente Jueces.

Solicitudes



*El sistema de registro durante el periodo de reporte no disponía de los mecanismos para filtrar por peticiones rechazadas. Se está trabajando para disponer de este dato en los próximos informes.

1. No hay datos disponibles porque este indicador se contabilizaba como solcitudes atípicas o de bajo volumen.
2. Este dato no es comparable con el resto de años ya que desde 2019 se ha considerado registrar las suspensiones a cuentas a individuales en este indicador (antes se reportaba como bloqueo de contenidos).



Chile

www.telefonicachile.cl



Accesos a cierre de 2021 (datos en miles).

El Grupo Telefónica en Chile es proveedor de servicios de telecomunicaciones (Banda Ancha, TV digital y Voz), y ha reorganizado su estructura societaria que culminó con el proceso de unificación de las marcas comerciales bajo el nombre de Movistar en octubre de 2009.

Telefónica Chile gestiona más de 10,7 millones de accesos a diciembre de 2021.

Respecto a las cifras financieras, los ingresos de Telefónica en Chile han alcanzado los 1.769 millones de euros y el OIBDA 920 millones de euros.



Información a cierre de 2021

Interceptación legal

Contexto legal

- N°5 del art 19 Constitución Política. Inviolabilidad de las comunicaciones.
- Código Procesal Penal, artículos 9, 219, 222, 223 y 224.
- Ley 20.000. Tráfico y control de Estupefacientes, artículo 24.
- Ley 19.913 sobre Lavado de dinero.
- Ley 18.314 que determina conductas terroristas. N°3, artículo 14.
- Decreto Ley 211, artículo 39 letra n).
- Ley 19.974. Ley Sistema Nacional de Inteligencia. Letras a), b), c) y d) de Artículo 24, en relación a los artículos 23 y 28 del mismo cuerpo legal.
- Código Procedimiento Penal, artículos 177, 113 bis y 113 ter.
- Decreto 142 de 2005 del Ministerio de Transportes y Telecomunicaciones, Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación.

Autoridades Competentes

- Persecutor Penal (Ministerio Público) en virtud de autorización judicial previa.
- Agencias de Inteligencia del Estado, mediante el Sistema Nacional de Inteligencia con autorización de Ministro de Corte de Apelaciones .
- Policías mediante autorización de Juez Instructor del Crimen (Procedimiento Penal Inquisitivo).
- Fiscalía Nacional Económica, mediante autorización previa de Tribunal de Defensa de Libre Competencia, aprobada por Ministro de Corte de Apelaciones respectivo.

Solicitudes



*Las bajas no se consideran dentro del total de solicitudes ya que son bajas que se producen de manera automática por encontrarse en la propia solicitud inicial el plazo para la interceptación.

Metadatos asociados a las comunicaciones

Contexto legal

- N° 4° del artículo 19 de la Constitución Política de la República de Chile, en conformidad a lo dispuesto en el artículo Único de la Ley 21.096: la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley.
- Código Procesal Penal: Inciso 5° del Artículo 222 del Artículo 222 Código Procesal Penal En relación al Artículo 180 del mismo cuerpo le- gal, bajo apercibimiento de Desacato, Artículo 240 Código Procedimiento Civil.
- Procedimiento penal inquisitivo: Artículo 120 bis y 171 del Código de Procedimiento Penal.





Autoridades Competentes

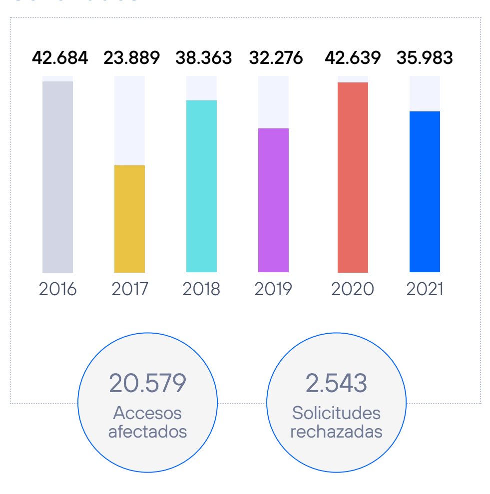
→ Persecutor Penal Público: Ministerio Público mediante Orden de Investigar sólo respecto de datos personales que no estén amparados por Garantías Constitucionales de Privacidad e Inviolabilidad de las Comunicaciones.

→ Policías con autorización del ministerio Público y orden de investigar.

→ Juez de Sumario en Procedimiento penal inquisitivo. (Código Procedimiento Penal).

→ Agencias de Inteligencia de Estado con autorización judicial previa.

Solicitudes



Bloqueo y restricción de contenidos

Contexto legal

→ Ley 17.336, sobre Propiedad Intelectual. Artículo 85 Q, en relación a lo dispuesto en el Artículo 85 R letras a) y b) del mismo cuerpo legal.

→ Código de Procedimiento Civil: Medidas precautorias o cautelares innominadas.

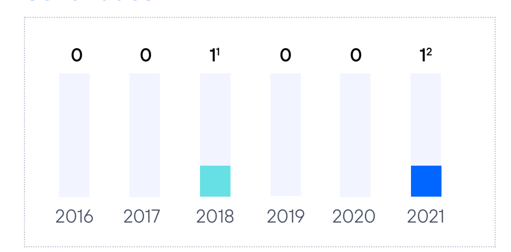
→ Código Procesal Penal: Medidas precautorias o cautelares innominadas.

Autoridades Competentes

→ Tribunales ordinarios y especiales dependientes orgánicamente del Poder Judicial.

→ Tribunal de Defensa de la Libre Competencia, sujeto a la superintendencia directiva, correccional y económica de la Corte Suprema, que estén conociendo de un proceso contencioso.

Solicitudes



1. Por violación de derechos de autor (Ley 17.336 de Propiedad Intelectual).

2. Se bloquea 1 URL y 2 direcciones IPs. Por propiedad intelectual

Suspensiones geográficas o temporales de servicio

Contexto legal

No existen leyes en el marco regulatorio que permitan suspensiones geográficas o temporales del servicio.

Autoridades Competentes

No aplica.

Solicitudes



Colombia

www.telefonica.co



Accesos a cierre de 2021 (datos en miles).

Telefónica tiene presencia en Colombia desde el año 2004. Comenzó con actividades en el mercado móvil, tras la adquisición de la operación celular de Bellsouth en el país. Posteriormente, en el año 2006, Telefónica adquirió el control y la gestión de Colombia Telecomunicaciones. Telefónica proporciona hoy en el país servicios de telecomunicaciones de voz, banda ancha y televisión de pago.

Telefónica Colombia gestiona mas de 21,9 millones de accesos a cierre de 2021.

Los ingresos de Telefónica en Colombia alcanzaron 1.312 millones de euros y el OIBDA sumó 413 millones de euros.



Información a cierre de 2021

Interceptación legal

Contexto legal

→ Constitución Colombiana, artículo 15 y 250.

→ Ley 599 de 2000 Código Penal y Ley 906 de 2004 Código de Procedimiento Penal art. 200 modificado por la ley 1142 de 2007 art.49 y art.235 modificado por la ley 1453 de 2011 art.52.

→ Ley 1621 de 2013. Ley de inteligencia y contrainteligencia, artículo 44.

→ Decreto 1704 de 2012, artículo 1-8. por medio del cual se reglamenta el artículo 52 de la ley 1453 de 2011, se deroga el decreto 075 de 2006 y se dictan otras disposiciones.

→ Decreto 2044 de 2013, art. 3 por el cual se reglamentan los artículos 12 y 68 de la ley 1341 de 2009.

→ Ley 1273 de 2009: por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, artículo 269C.

Autoridades Competentes

→ En Colombia la única autoridad competente para realizar interceptación de comunicaciones es la Fiscalía General de la Nación, a través del grupo de Policía Judicial de la mencionada entidad.

Solicitudes*



*Solicitudes sobre líneas fijas

Líneas moviles: No se reportan interceptaciones sobre líneas móviles: La Fiscalía General de la Nación en Colombia, por ser la autoridad competente de conformidad con la Constitución y la Ley, realiza las interceptaciones de manera directa sobre las líneas móviles.

Metadatos asociados a las comunicaciones

Contexto legal

→ Constitución Colombiana, artículo 250.

→ Ley 599 de 2000 Código Penal y Ley 906 de 2004 Código de Procedimiento Penal, artículo 200 modificado.

→ Ley 1621 de 2013, Ley de inteligencia y contrainteligencia, artículo 44.

→ Decreto 1704 de 2012, artículo 1-8. por medio del cual se reglamenta el artículo 52 de la ley 1453 de 2011, se deroga el decreto 075 de 2006 y se dictan otras disposiciones.

→ Sentencia C-336 de 2007 Corte constitucional.

→ Ley 1273 de 2009, artículo 269F, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Autoridades Competentes

Ley vigente aplicable es la 906 de 2004 Código de Procedimiento Penal.

Órganos de Indagación e investigación

a) Órganos art. 200 modificada ley 1142 de 2007:

Corresponde a la Fiscalía General de la Nación realizar la indagación e investigación de los hechos que revistan características de un delito que lleguen a su conocimiento por medio de denuncia, querella, petición especial o por cualquier otro medio idóneo.

b) Órganos de Policía Judicial Permanente art. 201 C.P.P.

Ejercen permanentemente las funciones de policía judicial los servidores investidos de esa función, pertenecientes al Cuerpo Técnico de Investigación de la Fiscalía General de la Nación, a la Policía Nacional y al Departamento Administrativo de Seguridad, por intermedio de sus dependencias especializadas.

En los lugares del territorio nacional donde no hubiere miembros de policía judicial de la Policía Nacional, estas funciones las podrá ejercer la Policía Nacional.

c) Órganos que ejercen funciones permanentes de policía Judicial de manera especial dentro de su competencia Art. 202 C.P.P.

Ejercen permanentemente funciones especializadas de policía judicial dentro del proceso penal y en el ámbito de su

competencia, los siguientes organismos:

1. La Procuraduría General de la Nación.

2. La Contraloría General de la República.

3. Las autoridades de tránsito.

4. Las entidades públicas que ejerzan funciones de vigilancia y control.

5. Los directores nacional y regional del Inpec, los directores de los establecimientos de reclusión y el personal de custodia y vigilancia, conforme con lo señalado en el Código Penitenciario y Carcelario.

6. Los alcaldes.

7. Los inspectores de policía.

Los directores de estas entidades, en coordinación con el Fiscal General de la Nación, determinarán los servidores públicos de su dependencia que integrarán las unidades correspondientes.

d)Órganos que ejercen transitoriamente funciones de policía judicial Art.203 CPP

Ejercen funciones de policía judicial, de manera transitoria, los entes públicos que, por resolución del Fiscal General de la Nación, hayan sido autorizados para ello. Estos deberán actuar conforme con las autorizaciones otorgadas y en los asuntos que hayan sido señalados en la respectiva resolución.

e) Órgano técnico científico Art.204 CPP

El Instituto Nacional de Medicina Legal y Ciencias Forenses, de conformidad con la ley y lo establecido en el estatuto orgánico de la Fiscalía General de la Nación, prestará auxilio y apoyo técnico-científico en las investigaciones desarrolladas por la Fiscalía General de la Nación y los organismos con funciones de policía judicial. Igualmente lo hará con el imputado o su defensor cuando estos lo soliciten.

La Fiscalía General de la Nación, el imputado o su defensor se apoyarán, cuando fuere necesario, en laboratorios privados nacionales o extranjeros o en los de universidades públicas o privadas, nacionales o extranjeras.

Solicitudes



Bloqueo y restricción de contenidos

Solicitudes*



*Desde septiembre de 2016 entró en operación la plataforma "WOLF Control de Contenidos" la cual filtra de manera especializada todo el contenido ilegal tipificado por las autoridades locales como por ejemplo pornografía infantil.

El listado se continua actualizando y publicando de manera periodica por medio de la página web del Ministerio de las Tecnologías de la Información y las Comunicaciones.

El procedimiento para validación de urls es:

1. Consulta de publicaciones en el portal del MinTic. Con esta consulta periódica se valida si existen o no nuevos URLs con orden de bloqueo.

2. Análisis de publicaciones de URLs. Si existen nuevos URLs se identifican y se cargan en la plataforma DPI (Deep Packet Inspection).

3. Análisis, bloqueo y desbloqueo de URLs. Si es necesario bloquear o desbloquear los URLs por las actualizaciones del listado, se genera una orden de trabajo para ser ejecutada por el área técnica.

4. Consulta de verificación. Ejecutada la orden de trabajo se valida que las URLs que tienen orden de bloqueo se encuentren bloqueadas.

El Ministerio de Tecnologías de la Información y las Comunicaciones se encargan de registrar en una plataforma el listado con las órdenes de bloqueo tanto de material de abuso infantil como de juegos en línea y cada operador es responsable de acceder a la plataforma, validar si hay órdenes nuevas y hacer el bloqueo respectivo

Material de abuso sexual infantil

Contexto legal

→ Ley 1098 de 2006 código de infancia y adolescencia y Ley 1453 de 2011reforma el Código de infancia y adolescencia.

→ Ley 679 de 2001: Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución Artículos 7 y 8.

→ Decreto 1524 de 2002: reglamentar el artículo 5 de la Ley 679 de 2001, con el fin de establecer las medidas técnicas y administrativas destinadas a prevenir el acceso de menores de edad a cualquier modalidad de información pornográfica contenida en Internet o en las distintas clases de redes informáticas a las cuales se tenga acceso mediante redes globales de información. Artículos 5 y 6.

→ Ley 1450 de 2011: Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014 Artículo 56.

→ Ley 1273 de 2009: por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones Artículo 269G, art. 269F.

→ Resolución CRC 3502 de 2011.

Autoridades Competentes

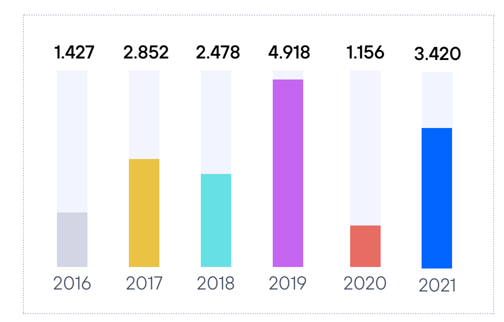
→ Policía Judicial con orden de juez de control de garantías.

→ Juez de Control de Garantías.

→ Autoridades Judiciales, con unidades de inteligencia y contrainteligencia (Policía Nacional, Fuerzas militares, UIAF).

La Policía Nacional le envía al Ministerio de las Tecnologías de la Información y las Comunicaciones un listado de URLs con orden de bloqueo para que el Ministerio lo publique en su página web y pueda ser consultado por los PSI. Para acceder a este listado, los PSI deben contar con un usuario y una contraseña que es suministrada previamente por el Ministerio, para evitar que cualquier persona pueda consultar los URLs que tienen orden de bloqueo por contener material de pornografía infantil.

Nº URL*



* Número de URLs agregados al listado publicado por MinTIC durante ese año.

Juegos Ilegales

Contexto legal

→ Ley 1753 de 2015: por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones Artículo 93, parrágrafo 3.

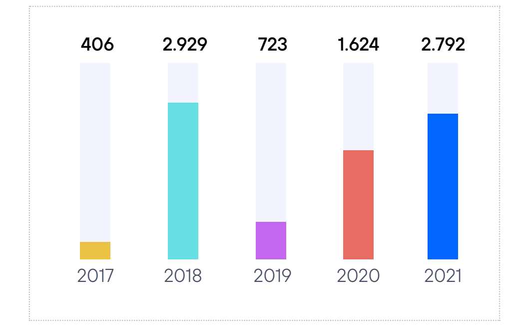
→ Ley 1450 de 2011, artículo 56.

→ Resolución CRC 3502 de 2011.

Autoridades Competentes

→ Coljuegos, empresa industrial y comercial del Estado encargada de la administración del monopolio rentistico de los juegos de suerte y azar, en conjunto con la Policía Nacional identifican portales Web en los que se comercializan juegos de suerte y azar no autorizados y le solicitan al Ministerio de las Tecnologías de la Información y las Comunicaciones que comunique a los PSI el listado de las URLs que deben bloquear.

Nº URL*



* Número de URLs agregados al listado publicado por MinTIC durante ese año.

Orden judicial

Contexto legal

→ Ley 599 de 2000 Código Penal y Ley 906 de 2004 Código de Procedimiento Penal.

→ Sentencia C-897 de 2005 Corte Constitucional.

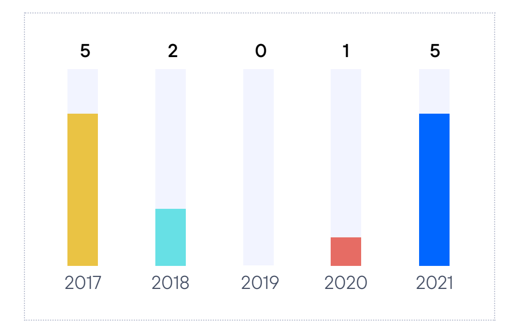
→ Sentencia C-600 de 2019 Corte Constitucional.

→ Sentencia C-243 de 1996 Corte Constitucional.

Autoridades Competentes

La Fiscalía General de la Nación y la Superintendencia de Industria y Comercio dentro de las investigaciones que adelantan le solicitan al Ministerio de las Tecnologías de la Información y las Comunicaciones que comunique a los PSI las URLs que deben bloquear.

Nº URL*



* Número de URLs agregados al listado publicado por MinTIC durante ese año.

Suspensiones geográficas o temporales de servicio

Contexto legal

→ Ley 1341 de 2009, artículo. 8. Casos de emergencia, conmoción o calamidad y prevención.

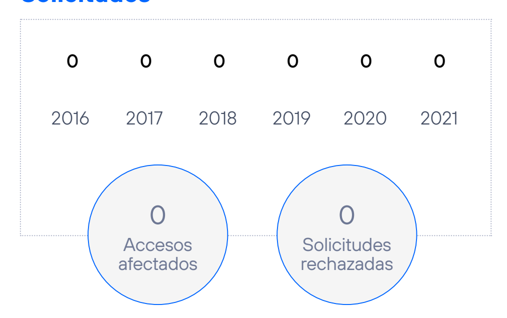
→ Decreto 2434 de 2015, Resolución CRC 4972 de 2016 – Obliga a priorizar las llamadas entre autoridades para atender emergencias.

Esta priorización implica terminar llamadas de usuarios que no están en el listado de números.

Autoridades Competentes

Se darán prelación a las autoridades en la transmisión de comunicaciones gratuitas y oportunas para efectos de prevención de desastres, cuando aquellas se consideren indispensables.

Solicitudes



Ecuador

www.telefonica.com.ec



Accesos

Telefonía fija	Telefonía móvil	Banda Ancha Fija	TV de pago
3	5.235	11	0,0

Accesos a cierre de 2021 (datos en miles).

En Ecuador, Telefónica inició sus operaciones en el 2004, con la adquisición de la operación móvil de BellSouth en el país (que en ese momento era el segundo operador ecuatoriano, con 816.000 clientes y una cuota del 35% del mercado).

Telefónica gestiona más de 5,2 millones de accesos en Ecuador a cierre de 2021.

Los ingresos ascendieron a 398 millones de euros y el OIBDA a 122 millones de euros.



Información a cierre de 2021

Interceptación legal

Contexto legal

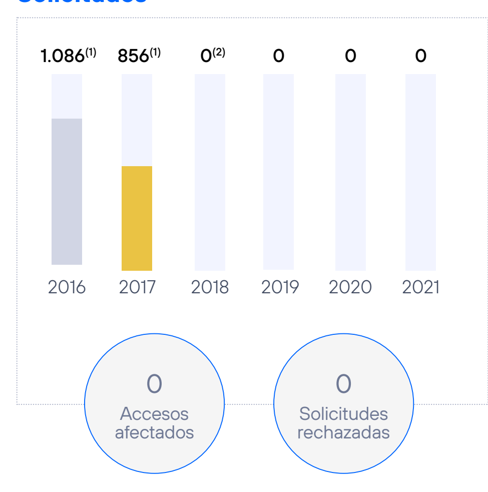
→Código Orgánico Integral Penal, artículo 476-477.

→Contrato de Concesión suscrito entre OTECEL S.A. y el Estado Ecuatoriano.

Autoridades Competentes

Fiscal competente dentro de una investigación.

Solicitudes



(1) Debido a un cambio de normativa, la fiscalía responde directamente sobre los pedidos de intervención y de datos en materia penal.

(2) Desde 2018 en adelante, la Fiscalía la única entidad autorizada a realizar este tipo de intercepción en tiempo real y la operadora no interviene en dicho proceso.

Metadatos asociados a las comunicaciones

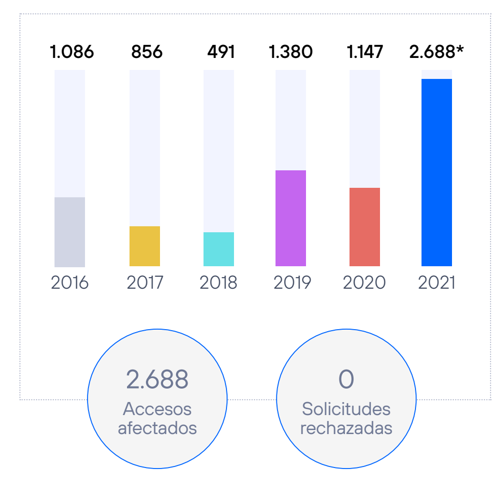
Contexto legal

→Código Orgánico Integral Penal, artículo 499.

Autoridades Competentes

→Jueces de Garantías Penales.

Solicitudes



* Gran parte de las peticiones del 2021 son expedientes retrasados del 2020 debido al Covid. La autoridad judicial y fiscal sufrió brotes de pandemia Covid (especialmente en Quito y Guayaquil).

Bloqueo y restricción de contenidos

Contexto legal

→Código Orgánico Integral Penal, artículo 583.

→Código Orgánico de la Economía Social de los Conocimientos, artículos 563 y 565.

Autoridades Competentes

→El Fiscal puede solicitar de manera fundamentada a Juez de Garantías penales autorización para proceder.

→SENADI (Servicio Nacional de Derechos Intelectuales puede ordenar medidas cautelares).

Solicitudes



*Por vulnerar derechos de propiedad intelectual.

Suspensiones geográficas o temporales de servicio

Contexto legal

Constitución del Ecuador, artículos 164 y 165.

Autoridades Competentes

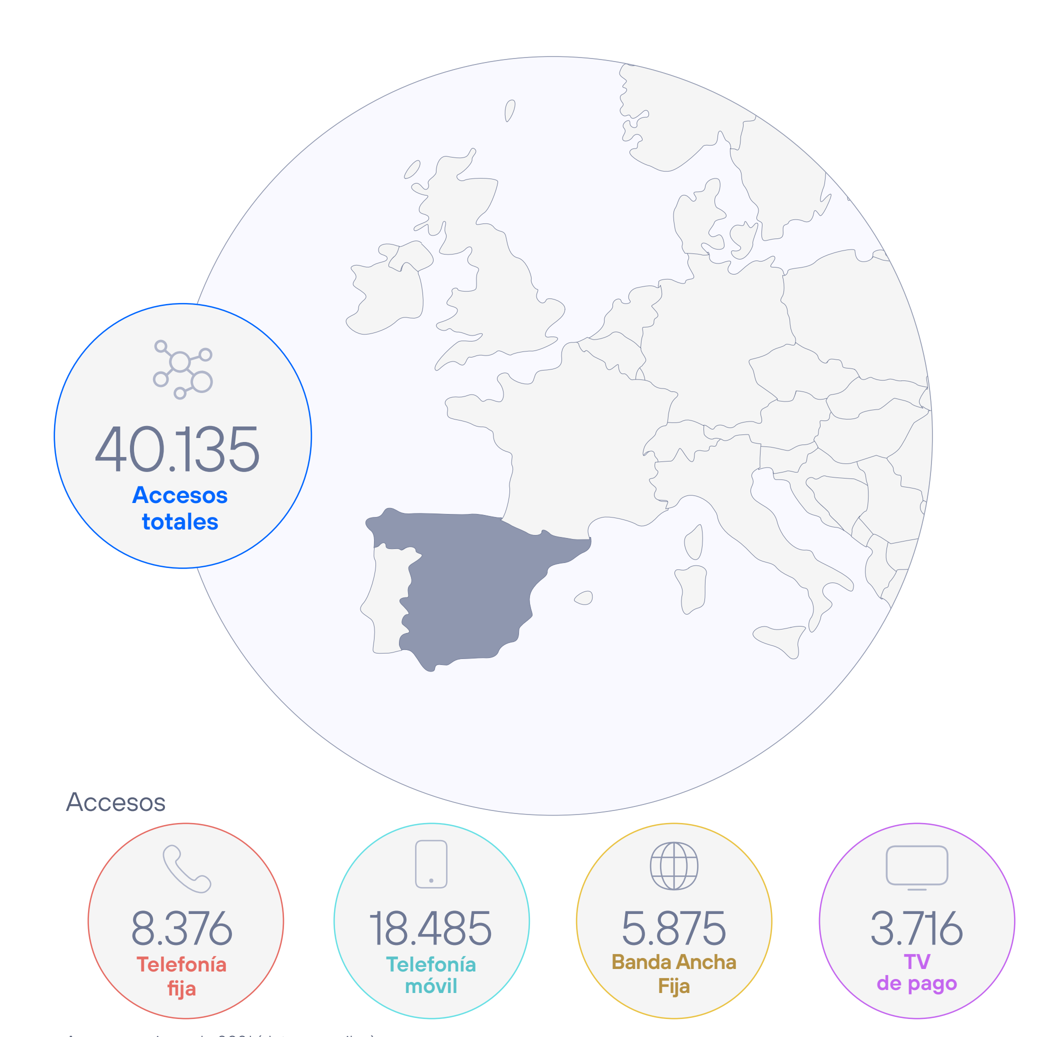
Aquella(s) que el Presidente de la República delegue en su nombre según las circunstancias que refleja la ley.

Solicitudes



España

www.telefonica.es



Accesos

8.376	18.485	5.875	3.716
Telefonía fija	Telefonía móvil	Banda Ancha Fija	TV de pago

Accesos a cierre de 2021 (datos en miles).

Telefónica desarrolla su actividad en España, principalmente en los negocios de telefonía fija y móvil, con la banda ancha como herramienta clave para el desarrollo de ambos, y en los servicios de TI y soluciones. Telefónica España es la compañía de telecomunicaciones líder en España por accesos, incluyendo voz, datos, televisión y acceso a internet y ofrece a sus clientes los más innovadores servicios y las tecnologías más punteras para conseguir el objetivo de convertirse en la primera telco digital.

Telefónica España gestiona más de 40,1 millones de accesos a cierre de 2021.

Los ingresos por operaciones totalizaron 12.417 millones de euros y el OIBDA alcanzó los 3.377 millones de euros en 2021.



Información a cierre de 2021

Interceptación legal

Contexto legal

→ Constitución Española, artículo 18.

→ Ley de enjuiciamiento Criminal, artículo 588.

→ Ley 9/2014, General de Telecomunicaciones, artículo 39 y 42. Además, esta ley ha sido modificada en virtud de lo establecido en el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Así existe una nueva redacción al apartado 6 del artículo 4 y al apartado 1 del artículo 81.

→ Apartado 6 del artículo 4, " El Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicas en determinados supuestos excepcionales que puedan afectar al orden público, la seguridad pública y la seguridad nacional. En concreto, esta facultad excepcional y transitoria de gestión directa o intervención podrá afectar a cualquier infraestructura, recurso asociado o elemento o nivel de la red o del servicio que resulte necesario para preservar o restablecer el orden público, la seguridad pública y la seguridad nacional.

Asimismo, en el caso de incumplimiento de las obligaciones de servicio público a las que se refiere el Título III de esta Ley, el Gobierno, previo informe preceptivo de la Comisión Nacional de los Mercados y de la Competencia, e igualmente con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa o la intervención de los correspondientes servicios o de la explotación de las correspondientes redes.

Los acuerdos de asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refieren los párrafos anteriores se adoptarán por el Gobierno por propia iniciativa o a instancia de una Administración Pública competente. En este último caso, será preciso que la Administración Pública tenga competencias en materia de seguridad o para la prestación de los servicios públicos afectados por el anormal funcionamiento del servicio o de la red de comunicaciones electrónicas. En el supuesto de que el procedimiento se inicie a instancia de una Administración distinta de la del Estado, aquella tendrá la consideración de interesada y podrá evacuar informe con carácter previo a la resolución final."

→ Apartado 1 del artículo 81, "Previamente al inicio del procedimiento sancionador, podrá ordenarse por el órgano competente del Ministerio de Economía y Empresa, mediante resolución sin audiencia previa, el cese de la presunta actividad infractora cuando existan razones de imperiosa urgencia basada en alguno de los siguientes supuestos:

a) Cuando exista una amenaza inmediata y grave para el orden público, la seguridad pública o la seguridad nacional.

b) Cuando exista una amenaza inmediata y grave para la salud pública.

c) Cuando de la supuesta actividad infractora puedan producirse perjuicios graves al funcionamiento de los servicios de seguridad pública, protección civil y de emergencias.

d) Cuando se interfiera gravemente a otros servicios o redes de comunicaciones electrónicas.

e) Cuando cree graves problemas económicos u operativos a otros proveedores o usuarios de redes o servicios de comunicaciones electrónicas o demás usuarios del espectro radioeléctrico.»

Autoridades Competentes

→ Jueces de los Juzgados de Instrucción

→ Casos excepcionales (urgencia, bandas armadas) el Ministro del Interior o el Secretario de Estado de Seguridad. En 24 horas el juez ratificará o revocará la solicitud

→ El Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicas en determinados supuestos excepcionales que puedan afectar al orden público, la seguridad pública y la seguridad nacional.

Solicitudes



Metadatos asociados a las comunicaciones

Contexto legal

→Ley 25/2007 de Conservación de Datos, artículos 1-10.

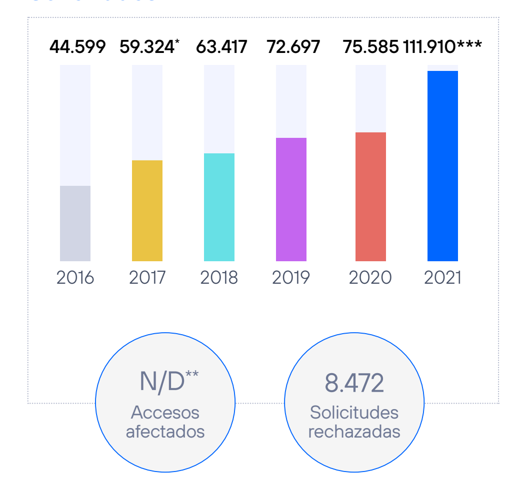
→Ley 9/14, General de Telecomunicaciones, artículos 39-42.

Autoridades Competentes

→Juzgados.

→Policía Judicial y Ministerio Fiscal (Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal).

Solicitudes



* En el año 2017 se puso en marcha un nuevo sistema de envío de mandamientos de las autoridades competentes por parte de las Fuerzas y Cuerpos de Seguridad del Estado, en el que cada petición de datos da lugar a un requerimiento individual. Con el sistema anterior, que aún está en funcionamiento para algunas Autoridades, un mismo mandamiento judicial puede dar lugar a múltiples solicitudes de datos, aunque se contabilice como una sola.

** La naturaleza de ciertos requerimientos y la configuración de las herramientas no permiten aportar este dato.

***El nuevo sistema de envío de mandamientos de las autoridades competentes [ver nota 1] se ha extendido y se ha generalizado el uso del sistema digital en 2021. En este sistema las peticiones tienden a ser por números de acceso, por lo que se reciben una cantidad mayor.

Bloqueo y restricción de contenidos

Contexto legal

→Real Decreto 1889/2011, artículos 22 y 23 por el que se regula el funcionamiento de la Comisión de Propiedad Intelectual, 30/12/2011.

→Texto Refundido de la Ley de Propiedad Intelectual, artículo 138, aprobado por el Real Decreto Legislativo 1/1996, 12/04/1996.

→Ley 34/2002, artículo 8, de servicios de la sociedad de la información y de comercio electrónico, 11/07/2002.

Autoridades Competentes

→Juzgados Mercantiles/Civiles/Cont.-Administrativo/Penal.

→Comisión de Propiedad Intelectual.

→Dirección General del Juego.

→Agencia Española del Medicamento y productos sanitarios.

Solicitudes



*Del total de solicitudes, tres se consideran continuas a lo largo del periodo de reporte. El motivo es la aplicación de procesos de bloqueos dinámicos, semanales y mensuales, autorizados judicialmente:

1) Sentencia de 11 de febrero de 2020 del Juzgado de lo Mercantil 7 de Madrid, que acordó estimar íntegramente la Demanda de TELEFÓNICA AUDIOVISUAL DIGITAL, S.L.U. (TAD), para proteger los contenidos de la Plataforma Movistar+. 2) Sentencias de los Juzgados de lo Mercantil n.º 2 y 8 de Barcelona, relativas a la Demanda presentada por los socios de MPA (Motion Picture Association).
3) Protocolo, bajo impulso del Ministerio de Cultura, para el refuerzo de la protección de los derechos de la propiedad intelectual, que desarrolla la aplicación de sentencias y autos judiciales. Todas habilitan para que se elabore y envíe, semanal y mensualmente, un listado con URLs/Dominios, que los Operadores de Telecomunicaciones/Proveedores de acceso a Internet de España, deben bloquear o desbloquear, según se solicite.

Suspensiones geográficas o temporales de servicio

Contexto legal
No existen leyes en el marco regulatorio que permitan suspensiones geográficas o temporales del servicio.

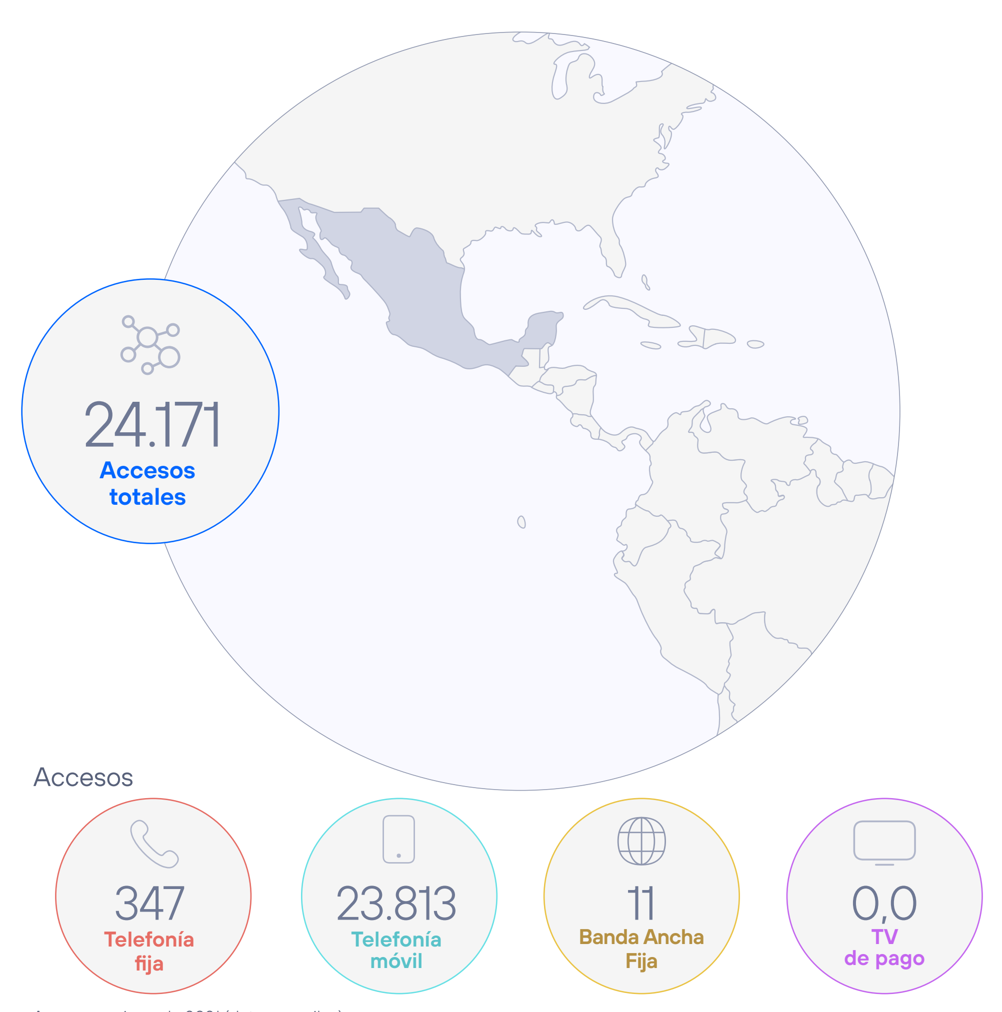
Autoridades Competentes
No aplica.

Solicitudes



México

www.telefonica.com.mx



24.171
Accesos totales

Accesos

Telefonía fija	Telefonía móvil	Banda Ancha Fija	TV de pago
347	23.813	11	0,0

Accesos a cierre de 2021 (datos en miles).

Telefónica México participa y compite en el mercado de las telecomunicaciones desde 2001 e impulsa el desarrollo de las telecomunicaciones en el país. Hoy cuenta con la mejor cobertura nacional, con más de 93 mil localidades, 90 mil kilómetros carreteros y más de 25.2 millones de clientes.

Las ofertas comerciales se encuentran disponibles en 315 Centros de Atención a Clientes (CAC), y más de 4.200 puntos de venta indirecta en todo el país.

Telefónica en Mexico gestiona más de 24,1 millones de accesos a cierre de 2021.

Respecto a las cifras financieras, los ingresos de Telefónica en Mexico alcanzaron 1.010 millones de euros y el OIBDA fue de 82 millones de euros.



Información a cierre de 2021

Interceptación legal

Contexto legal

- Constitución Política de los Estados Unidos Mexicanos, artículo 16, párrafo 12.
- Código Nacional de Procedimientos Penales, artículo 291.
- Ley Federal Contra la Delincuencia Organizada, artículo 16.

Autoridades Competentes

La autoridad judicial federal es quien determina si es procedente la solicitud de la autoridad investigadora respecto a la intervención de comunicaciones, quien ordena al concesionario establecer la medida por un tiempo determinado.

Solicitudes*



*Por razones técnicas las solicitudes se contabilizan como peticiones

Metadatos asociados a las comunicaciones

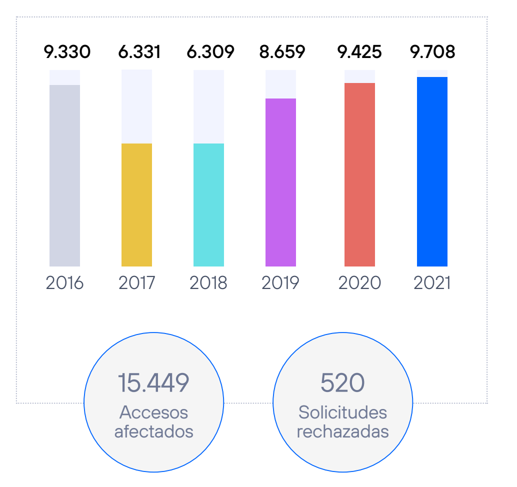
Contexto legal

- Ley Federal de Telecomunicaciones y Radiodifusión, artículo 190.
- Código Nacional de Procedimientos Penales, artículo 303.
- Ley de Vías Generales de Comunicaciones, artículo 122.

Autoridades Competentes

Los titulares de las instancias de seguridad y procuración de justicia designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación.

Solicitudes



Bloqueo y restricción de contenidos

Contexto legal

No existen leyes en el marco regulatorio que permitan bloqueo y restricción de contenidos.

Autoridades Competentes

No aplica.

Solicitudes



N/A	N/A	N/A	N/A	N/A	N/A
2016	2017	2018	2019	2020	2021

0 URL afectadas

0 Solicitudes rechazadas

Suspensiones geográficas o temporales de servicio

Contexto legal

No existen leyes en el marco regulatorio que permitan suspensiones geográficas o temporales del servicio.

Autoridades Competentes

No aplica.

Solicitudes

N/A	N/A	N/A	N/A	N/A	N/A
2016	2017	2018	2019	2020	2021

0 Accesos afectados

0 Solicitudes rechazadas

Perú

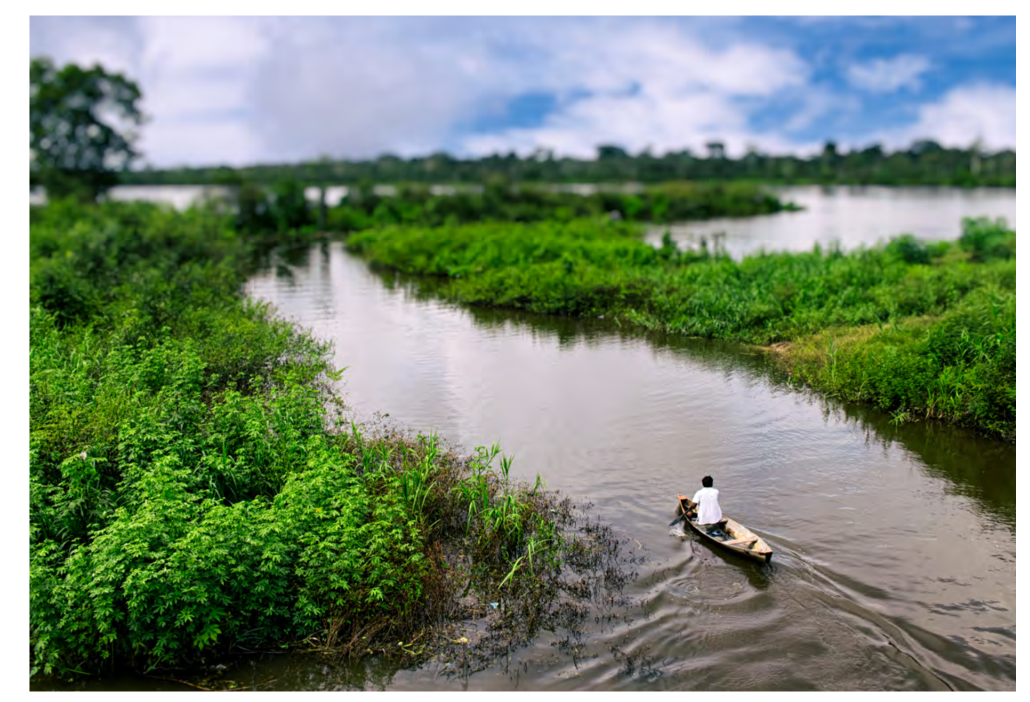
www.telefonica.com.pe



Accesos a cierre de 2021 (datos en miles).

Telefónica comenzó a operar en el mercado peruano a mediados de la década de los 90. Telefónica en Perú gestiona más de 16,9 millones de accesos en diciembre de 2021.

Respecto a las cifras financieras, los ingresos de Telefónica en Perú alcanzaron 1.533 millones de euros y el OIBDA sumó 252 millones de euros.



Información a cierre de 2021

Interceptación legal

Contexto legal

→ Constitución Política del Perú, artículo 2° inciso 10.

→ Ley de Telecomunicaciones (Decreto Supremo N° 013-93-TCC – Artículo 4°) y su Reglamento (Decreto Supremo N° 020-2007-MTC – Artículo 13°).

→ Ley N° 27697: Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional.

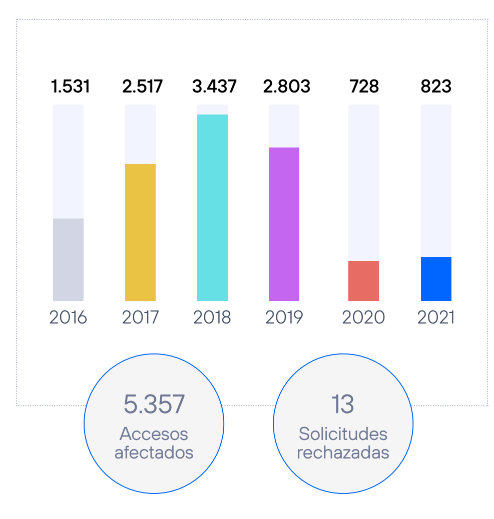
En todos los contratos de concesión existe la cláusula referida al secreto de las telecomunicaciones y protección de datos personales que establece que la empresa salvaguardará los mismos y mantendrá la confidencialidad de la información personal relativa a sus clientes, salvo que exista una orden judicial específica.

Autoridades Competentes

→ Juez (Poder Judicial).

→ Fiscal de la Nación, Fiscales Penales (Ministerio Público) con autorización del Juez.

Solicitudes*



*Se incluyen altas, prorrogas y cese de interceptaciones.

Por razones técnicas las solicitudes se contabilizan como peticiones

Metadatos asociados a las comunicaciones

Contexto legal

→ Constitución Política del Perú, artículo 2° inciso 10.

→ Ley de Telecomunicaciones (Decreto Supremo N° 013-93-TCC – artículo 4°) y su Reglamento (Decreto Supremo N° 020-2007-MTC – Artículo 13°).

→ Ley N° 27697: Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional.

→ Ley N° 31284: información de Geolocalización de los IMEI.

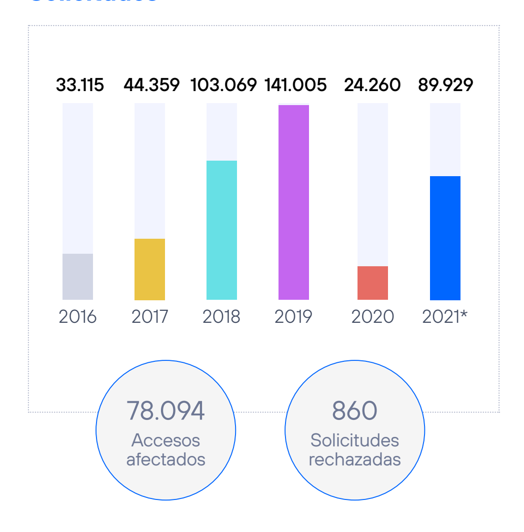
→ Decreto Legislativo N° 1182 que regula el uso de las Telecomunicaciones para la Identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado.

En todos los contratos de concesión existe la cláusula referida al secreto de las telecomunicaciones y protección de datos personales que establece que la empresa salvaguardará los mismos y mantendrá la confidencialidad de la información personal relativa a sus clientes, salvo que exista una orden judicial específica.

Autoridades Competentes

Los titulares de las instancias del Poder Judicial, Ministerio Público y Policía Nacional designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente.

Solicitudes



*Esta cifra incluye geolocalización y reportes de llamadas

Bloqueo y restricción de contenidos

Contexto legal

Ley de Derechos de Autor

Autoridades Competentes

→ INDECOPI (Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual).

En estricto, no ha habido un cambio legislativo, no existe alguna autoridad que pueda bloquear contenidos web, salvo el Poder Judicial. Sin embargo, existe una excepción en el caso de INDECOPI. Y es que, en virtud del artículo 169 de la Ley de Derechos de Autor, la Comisión de Derechos de Autor del INDECOPI tiene competencia para dictar medidas preventivas o cautelares y sancionar de oficio a solicitud de parte, las infracciones o violaciones a la legislación nacional de derechos de autor y derechos conexos; pudiendo amonestar, incautar, decomisar, disponer el cierre temporal o definitivo de los establecimientos donde se cometa la infracción.

Para el Indecopi, en la medida que a través de los sitios web se estaría realizando actos que vulneran el derecho de comunicación pública de las empresas denunciantes, la administración puede ordenar el bloqueo del acceso en territorio peruano al sitio web infractor, mediante el bloqueo basado en DNS y el bloqueo basado en URL.

Solicitudes*



*Requerimientos de INDECOPI (medidas cautelares en casos por propiedad intelectual).

Suspensiones geográficas o temporales de servicio

Contexto legal

Reglamento de la Ley de Telecomunicaciones (D.S. N° 020-2007-MTC - artículos 18° y 19°).

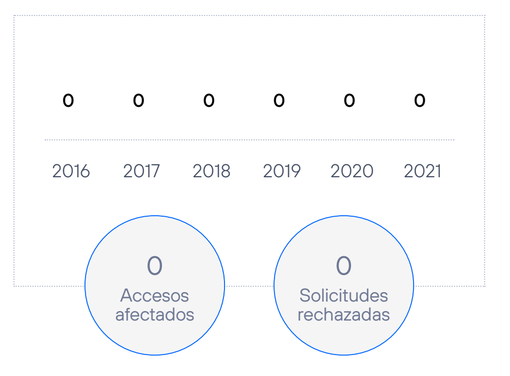
En los contratos de concesión se prevé que en caso de emergencia, crisis y seguridad nacional la empresa concesionaria brindará los servicios de telecomunicaciones priorizando las acciones de apoyo al Estado y siguiendo las instrucciones del MTC.

Autoridades Competentes

→ Ministerio de Transportes y Comunicaciones (MTC).

→ Sistema de Defensa Nacional y Civil.

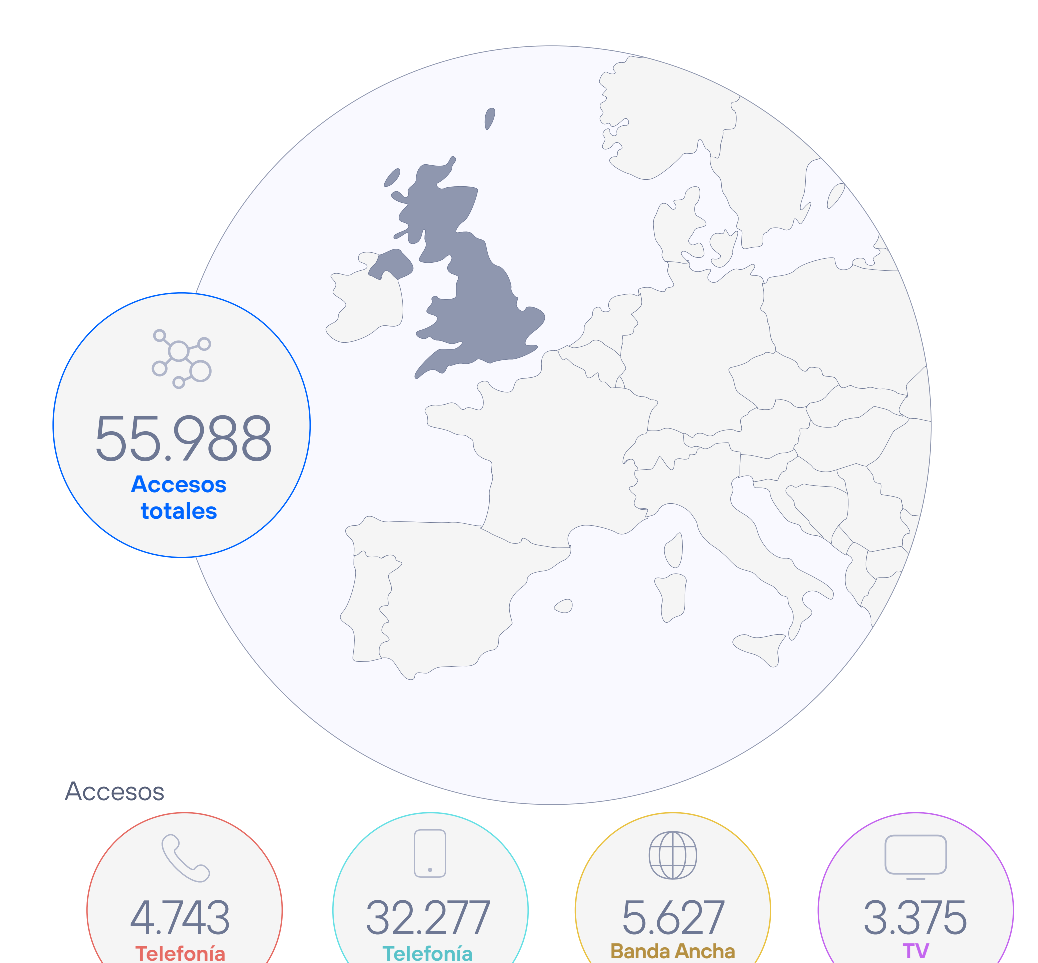
Solicitudes





Reino Unido

www.telefonica.com/en



55.988
Accesos totales

Accesos

4.743 Telefonía fija

32.277 Telefonía móvil

5.627 Banda Ancha Fija

3.375 TV de pago

Accesos a cierre de 2021 (datos en miles).

Telefónica comienza a operar en el Reino Unido a principios del 2006 tras adquirir O2, que se convierte en la marca comercial de Telefónica UK Limited.

La compañía ofrece un amplio abanico de productos y servicios de telefonía móvil sobre sus redes 2G, 3G, 4G y 5G. Además, O2 es propietaria de 50% de Tesco Mobile, así como de O2-Wifi.

En mayo de 2021 Liberty Global(Virgin Media) y Telefónica cerraron un acuerdo para fusionar sus negocios en el Reino Unido. Se trata de una de las operaciones más relevantes de la historia del Grupo Telefónica.

Se cuenta con más de 55,9 millones de accesos en Reino Unido a cierre de 2021.

Respecto a las cifras financieras, Los ingresos totales se sitúan en 2.628 millones de euros y el OIBDA en 919 millones de euros.

La transacción entre O2 y Virgin Media en 2021 ha sido, hasta el momento, una de las operaciones más relevantes de la historia del Grupo Telefónica. Tras alcanzar un acuerdo con Liberty Global el 07 de mayo del 2020 para unir los respectivos negocios en el Reino Unido y formar una joint venture (JV) participada al 50% por ambas compañías, el 01 de junio de 2021 se completó la transacción, una vez obtenidas las aprobaciones regulatorias pertinentes, llevadas a cabo las recapitalizaciones necesarias y cumplidas el resto de las condiciones pactadas para el cierre de la mencionada transacción.



Datos reportados son hasta la creación de la JV (01/06/2021).

Interceptación legal

Contexto legal

A lo largo de 2018, las provisiones de interceptación legal bajo el Reglamento de Instrucción Powers Act 2000 (RIPA) y la Inteligencia Ley de Servicios de 1994 (ISA) fueron reemplazadas por la Ley de Facultades de Investigación de 2016 (IPA). Este proceso se completó en noviembre de 2018.

La Comisión de Facultades de Investigación (IPC) está completamente establecida y el Departamento de Investigación Oficina de la Comisión de Poderes (IPCO) ha reemplazado a la Intercepción de Comunicaciones Oficina del Comisionado (IOCCO). La función de IPCO es supervisar la implementación y el cumplimiento con las solicitudes de interceptación legal realizadas conforme a la IPA.

Autoridades Competentes

Los principios de RIPA se han continuado bajo la IPA pero con supervisión adicional del poder Judicial. Bajo la IPA, el Secretario de Estado de departamento gubernamental relevante puede emitir una orden de intercepción cuando él/ella crea que es necesario en pro del interés de seguridad nacional, con el fin de prevenir o detectar delitos graves o con el propósito de salvaguardar la economía bienestar del Reino Unido.

Actualmente, en el Reino Unido hay ocho agencias autorizadas que pueden solicitar la emisión de una orden por parte de la Secretaría de Estado. Son:

- una persona que es jefe de un servicio de inteligencia;
- el Director General de la Agencia nacional contra la delincuencia;
- el Comisario de la Policía municipal;
- el Jefe de policía del Servicio de Policía de Irlanda del Norte;
- el Jefe de Policía del Servicio de Policía de Escocia;
- los comisionados de la Agencia Tributaria y de Aduanas de Su Majestad;
- el Jefe de Inteligencia para la Defensa; y
- una persona que es la autoridad competente de un país o territorio fuera del Reino Unido a los efectos de un dispositivo de asistencia mutua de la UE o de un acuerdo internacional de asistencia mutua.

Para obtener una orden de interceptación legal, la autoridad solicitante debe enviar una solicitud al correspondiente Secretario de Estado. El Secretario de Estado debe considerar, para decidir si emite la orden, si (entre otras cosas) existen fundamentos para justificar la emisión de la orden (ver más arriba) y si la interceptación autorizada por la orden es proporcionada a lo que se busca conseguir con dicha interceptación.

A partir de noviembre de 2018, todas las solicitudes de interceptación legal se han realizado de conformidad con la Ley de Protección de la Propiedad Intelectual y deben ser autorizadas por el Secretario de Estado (o su adjunto) en forma de una orden judicial y un juez. El juez considerará los mismos factores que el Secretario de Estado (es decir, si hay motivos para emitir la orden y si la conducta es proporcional al objetivo).

Solicitudes*



*La sección 57 de la IPA prohíbe la divulgación de la existencia de cualquier orden de interceptación legal salvo en circunstancias excepcionales según la sección 58 de la IPA.

La OIPC elabora un informe anual sobre la adquisición y divulgación de datos de comunicaciones por parte de los organismos de inteligencia, las fuerzas de policía y otras autoridades públicas. En él se dan detalles de las cifras globales, pero no por empresa. Véase: https://www.ipco.org.uk/publications/annual-reports/

Metadatos asociados a las comunicaciones

Contexto legal

Las disposiciones para la divulgación de datos de comunicaciones bajo RIPA e ISA, y la Ley de Seguridad y Contra el Terrorismo de 2015 (CTSA) fueron reemplazadas por la IPA en febrero de 2019.

La provisión para la retención de datos de comunicaciones, previamente retenida bajo la Ley de Poderes de Investigación de Retención de Datos 2014 (DRIPA 2014), ahora se realiza bajo la sección 87 de IPA.

Autoridades Competentes

En virtud del artículo 61 de la IPA, un alto funcionario designado de una autoridad pública pertinente puede autorizar la divulgación de datos. De manera similar a la RIPA, según la IPA, las personas que pueden autorizar la divulgación de datos suelen ser altos funcionarios de policía u otros altos funcionarios de los servicios de seguridad pertinentes. Estos funcionarios, salvo en situaciones de urgencia, estarán obligados a obtener una autorización previa de la Oficina de Autorizaciones de Datos de Comunicaciones, que tomará una decisión independiente sobre si conceder o rechazar las solicitudes de datos de comunicaciones.

Solicitudes*



*El apartado 82 de la IPA tipifica como delito la divulgación de detalles de solicitudes de datos de comunicación.

Como se indicó anteriormente, IPCO produce un informe anual, que brinda el número total de la industria. Los números de empresas individuales no se divulgan.

Bloqueo y restricción de contenidos

Contexto legal

- Apartado 97A de la Ley de 1988 sobre derechos de autor, diseños y patentes.
- S.37 (1) Senior Courts Act 1981.
- Artículo 11 de la Directiva sobre la Protección de la Propiedad Intelectual.

El único filtrado de contenido que el gobierno del Reino Unido espera de los operadores móviles y de banda ancha del Reino Unido (salvo cuando se emite una orden judicial), es el uso de la lista de bloqueo de Internet Watch Foundation (IWF) para sitios ilegales de abuso infantil. Esto es parte de un acuerdo en la comunidad policial para prevenir la explotación infantil. Esto no es un requisito legal. En 2004, Telefónica Reino Unido fue uno de los fundadores firmantes del código de prácticas de protección infantil de los operadores móviles del Reino Unido para la autorregulación de nuevas formas de contenido en móviles. Este Código también explica que bloquearemos voluntariamente el acceso a contenido clasificado para mayores de 18, a menos que un cliente haya confirmado que es mayor de 18 años. Este contenido es legal. P.ej. sitios legales para adultos (a diferencia de los sitios IWF que son sitios de abuso infantil).

La existencia de este código y su cumplimiento por parte de los operadores móviles del Reino Unido es inusual. Es inusual en el sentido de que no es algo (hasta donde sabemos) que se replica en otros países y también en el sentido de que no es vinculante pero aún así los operadores móviles lo cumplen.

Puede consultar el código aqui: http://www.mobilebroadbandgroup.com/documents/mbg_content_code_v2_100609.pdf

Autoridades Competentes

- Internet Watch Foundation.
- Tribunales.

Solicitudes*



*Solo la IWF, las estadísticas no están disponibles.

En 2021, Virgin media recibió 6 solicitudes de bloquear sitios web por infracción de la propiedad intelectual



Suspensiones geográficas o temporales de servicio

Contexto legal

Telefónica UK está obligada a limitar el servicio en situaciones de sobrecarga de la red (por ejemplo en grandes catástrofes, etc.) para priorizar los servicios de respuesta a emergencias. El esquema de acceso preferente de telecomunicaciones móviles (MTPAS) se creó bajo la Ley de 2004 sobre contingencias civiles (CCA). La elegibilidad está restringida a las organizaciones que tienen un papel para responder a, o recuperarse de, una emergencia tal como se define en la CCA.

Al inicio de una respuesta a una emergencia, el jefe de policía pertinente seguirá el protocolo acordado para notificar a todos los operadores de red móvil que se ha producido un incidente grave y solicitar la monitorización de los niveles de tráfico de llamadas. Si la red se congestiona, se solicitará a los operadores de red que consideren la posibilidad de acogerse a la MTPAS para facilitar que los equipos de emergencia realicen llamadas con prioridad sobre otros clientes.

Autoridades Competentes

- → El jefe de policía pertinente seguirá el protocolo acordado.
- → La suspensión del servicio se negocia entre las autoridades de emergencias y los CSP, y Telefónica UK puede oponerse si cree que la acción no impactaría la carga de red.

Solicitudes



Uruguay

www.telefonica.com.uy



Accesos a cierre de 2021 (datos en miles).

Telefónica está presente en Uruguay desde 2005.

En 2021 Los ingresos de Telefónica en Uruguay alcanzaron los 184 millones de euros y el OIBDA sumó 75 millones de euros.



Información a cierre de 2021

Interceptación legal

Contexto legal

→Constitución de la República, artículo 28.

→Ley 18.494, artículo 5.

→Decreto reservado de fecha 13 de marzo de 2014.

→Decreto 214 del Ministerio del Interior de 26 de octubre del 2021.

Autoridades Competentes

→Jueces penales a cargo de una investigación, previa solicitud del Ministerio Público y a través de la UNATEC (órgano del Ministerio del Interior encargado de centralizar dichas solicitudes).

Solicitudes



Metadatos asociados a las comunicaciones

Contexto legal

→Constitución de la República, artículo 28.

→Ley 18.494, artículo 5.

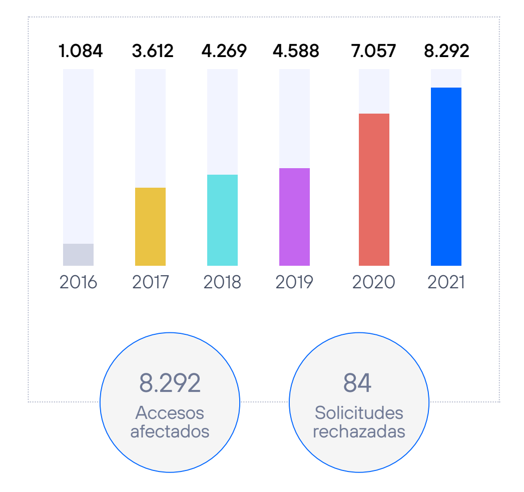
→Decreto reservado de fecha 13 de marzo de 2014.

→Decreto 214 del Ministerio del Interior de 26 de octubre del 2021.

Autoridades Competentes

→Jueces, mediante solicitud escrita y fundada.

Solicitudes*



* El incremento respecto al 2016 se corresponde porque a partir de 2017 se cuenta con una herramienta que permite contabilizar los requerimientos por cada cliente afectado. Hasta entonces un mismo requerimiento (oficio judicial) contenía más de un cliente afectado. A partir del 2017 cada requerimiento se corresponde a un cliente afectado. Por tanto, se debe al cambio en el criterio de contabilización.

Bloqueo y restricción de contenidos

Contexto legal

→ Ley 19.535 del 25 de septiembre de 2017, artículos 244 y 245.

→ Decreto 366/2017 reglamentó lo dispuesto por el artículo 244 y 245 de la Ley 19.535, 21/12/2017.

Autoridades Competentes

Se faculta al Poder Ejecutivo a adoptar las medidas preventivas y sancionatorias necesarias para evitar la proliferación de actividades de comercialización de juegos a través de internet, en especial el bloqueo de acceso a sitios web.

Solicitudes*



*Juegos y apuestas deportivas por internet

Suspensiones geográficas o temporales de servicio

Contexto legal

Ley 19.355, artículo 166: habilita al Ministerio del Interior a bloquear el ingreso de llamadas provenientes de servicios telefónicos al Servicio de Emergencia 911 cuando existan registros debidamente documentados que acrediten el uso irregular de las referidas comunicaciones en forma reiterada (más de tres comunicaciones en el mes o seis en el año).

Autoridades Competentes

Ministerio del Interior (Poder Ejecutivo).

Solicitudes*



*Suspensión temporal por un periodo de entre 3 y 6 meses.

Venezuela

www.telefonica.com.ve



Accesos a cierre de 2021 (datos en miles).

El Grupo Telefónica opera servicios de telefonía móvil en Venezuela desde el año 2005.

La Compañía tiene en Venezuela una oferta integral de servicios con productos en Internet móvil, televisión satelital y telefonía móvil y fija.

En 2021, los ingresos de Telefónica en Venezuela ascienden a 82 millones de euros y el OIBDA suma 40 millones de euros.



Información a cierre de 2021

Interceptación legal

Contexto legal

→Código Orgánico Procesal Penal, art. 205, 206.

→Decreto con Rango, Valor y Fuerza de Ley Orgánica del Servicio de Policía de Investigación, el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas y el Servicio Nacional de Medicina y Ciencias Forenses, art. 42.

Autoridades Competentes

→El Ministerio Publico a través de sus fiscales.

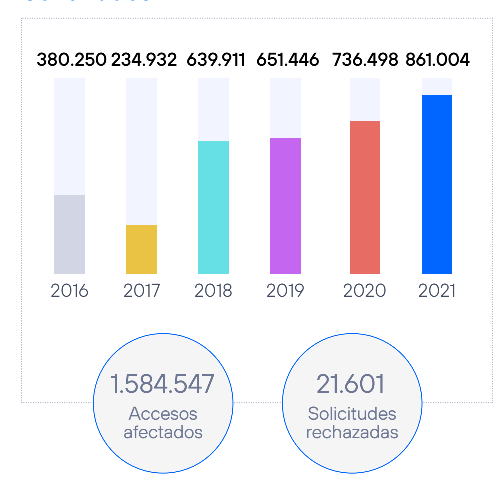
→Cuerpo de Investigaciones Científicas y Criminalísticas.

→El Servicio Bolivariano de Inteligencia Nacional (previa solicitud del Ministerio Público y autorización del juez correspondiente).

→Los cuerpos de policía debidamente habilitados para ejercer atribuciones en materia de investigación penal.

→Universidad Nacional Experimental de la Seguridad (UNES); demás órganos y entes especiales de investigación penal.

Solicitudes*



*No existen solicitudes de prorrogas y cese porque las únicas intervenciones que se realizan son solo las de ubicación y datos del suscriptor en tiempo real.

Metadatos asociados a las comunicaciones

Contexto legal

→Providencia Administrativa N° 171. Normas relativas a la recopilación o captación de datos personales de los solicitantes de los servicios de telefonía móvil y telefonía fija a través de redes inalámbricas o número no geográfico con servicio de voz nómada.

→Ley contra el Secuestro y la Extorsión, artículo 29.

Autoridades Competentes

→El Ministerio Público.

→El Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC).

→Los componentes de la Fuerza Armada Nacional Bolivariana, dentro de los límites de su competencia.

→Autoridades de inteligencia policial.

→El Cuerpo de Policía Nacional dentro del límite de sus funciones auxiliares de investigación penal.

→Cualquier otro órgano auxiliar de investigación penal cuya intervención sea requerida por el Ministerio Público.

Solicitudes



Bloqueo y restricción de contenidos

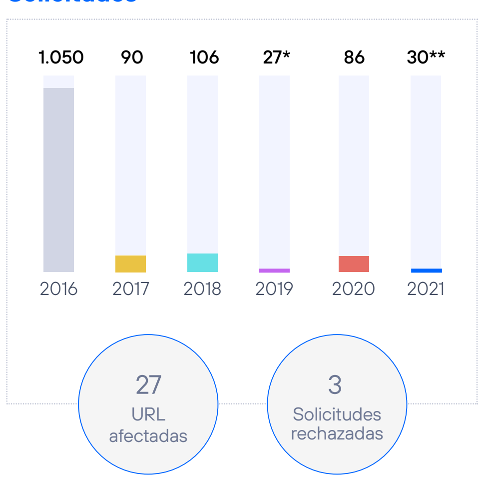
Contexto legal

- Ley Orgánica de Telecomunicaciones, artículo 5.
- Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos, artículo 27.

Autoridades Competentes

Comisión Nacional de Telecomunicaciones (CONATEL).

Solicitudes



*Sitios de juegos y apuestas por Internet.

**URLs afectados: 27 (cada solicitud contiene una sola petición, 3 solicitudes de bloqueos ya fueron previamente implementados).

Tipología: No hay detalle.

Solicitudes rechazadas: 3

Suspensiones geográficas o temporales de servicio

Contexto legal

La Ley Orgánica de Telecomunicaciones, artículo 5.

Autoridades Competentes

- Ministerio de Transportes y Comunicaciones (MTC).
- Sistema de Defensa Nacional y Civil.

Solicitudes





Glosario

CONCEPTO	EXPLICACIÓN
Autoridad competente	Jueces y Tribunales, Fuerzas y Cuerpos de Seguridad del Estado y demás administraciones u organismos gubernamentales a los que la ley faculta para realizar las peticiones objeto de este informe. Las Autoridades Competentes podrán variar en función del tipo de petición y de la legislación aplicable en cada uno de los países.
Datos personales	Se entiende por datos personales cualquier información que se refiera a alguna persona identificada o identificable, como puede ser su nombre, domicilio, destinatarios de sus comunicaciones, localización, contenido de las comunicaciones, datos de tráfico (días, hora, destinatarios de las comunicaciones, etc.).
Datos de localización	Los datos de localización pueden referirse a la latitud, la longitud y la altitud del equipo terminal del usuario, a la dirección de la marcha, al nivel de precisión de la información de la localización, a la identificación de la célula de Red en la que está localizado el equipo terminal en un determinado momento o a la hora en que la información de localización ha sido registrada.
Datos de tráfico	Cualquier dato tratado a efectos de la conducción de una comunicación a través de una Red de comunicaciones electrónicas o a efectos de su facturación.
DPI	Son las siglas en inglés de *Deep Packet Inspection* o inspección profunda de paquetes. DPI identifica situaciones de falta de cumplimiento de protocolos técnicos, virus, *spam*, o invasiones, aunque también puede usar criterios predefinidos diferentes a los anotados para decidir si algún paquete puede o no pasar, o requiere ser enrutado a un destino distinto, darle otra prioridad o asignación de ancho de banda, para tomar información con propósitos estadísticos o simplemente para eliminarlo.
IMEI	Son las siglas en inglés de *International Mobile Station Equipment Identity* o identidad internacional del equipamiento móvil. Se trata de un número de serie que identifica al terminal físicamente. El IMEI le sirve al operador para identificar terminales válidos y que, por tanto, pueden conectarse a la Red.
IMSI	Son las siglas en inglés de *International Mobile Subscriber Identity* o identidad internacional de abonado móvil. Es el identificador de la línea o servicio. Este número sirve para enrutar las llamadas y se puede obtener el país o la Red a la que pertenece.
IOCCO	Son las siglas en Inglés de *Interception of Communications Commissioner's* Office en Reino Unido. Es responsable de mantener bajo revisión la interceptación de comunicaciones, la adquisición y divulgación de datos de comunicaciones por agencias de inteligencia, fuerzas policiales y otras autoridades públicas. Presentan informes semestrales al Primer Ministro con respecto a la ejecución de las funciones del Comisionado de Interceptación de Comunicaciones.
MAJOR EVENTS	Existen ciertas situaciones de fuerza mayor que pueden provocar las siguientes actuaciones: 1. Restricción o denegación del servicio. (Incluyendo SMS, voz, correo electrónico, correo de voz, internet u otros servicios) que supone limitar la libertad de expresión. Ejemplos: → Restricción o denegación del servicio a nivel nacional. → Restricción o denegación de acceso a un sitio web(s) por motivos políticos (por ejemplo, páginas de Facebook; web de noticias –Ej. bbc.co.uk–; sitios web del partido de la oposición en el período previo a las elecciones; sitios web de grupos de derechos humanos, etc.).

CONCEPTO	EXPLICACIÓN
MAJOR EVENTS (cont.)	→ Desconexión específica de cualquier servicio de telecomunicaciones por motivos políticos. (Ej. en uno o un pequeño número de celdas). → Denegación de acceso a redes o a determinados servicios a ciertos clientes con el objetivo de limitar la libertad de expresión legítima de ese individuo. **2. Apagado de Red/control de acceso.** Ejemplos: → El cierre de toda la red a nivel nacional. → Control de acceso a la red en un área específica o en una región por motivos políticos. **3. La interceptación sin fundamento legal.** Situaciones en las que las autoridades interceptan comunicaciones sin tener una base legal por causas de fuerza mayor. **4. Comunicaciones impuestas por las autoridades.** Ejemplo: → Envío de mensajes/comunicaciones a nuestros clientes en nombre de un gobierno o agencia gubernamental por motivos políticos. **5. Cambios operacionales significativos.** Ejemplos: → Cambios, o propuestas de cambios, significativos operativos y técnicos respecto a los servicios de vigilancia (acceso a los datos, retención de datos e interceptación), que tienen como objetivo reducir el control por parte del operador para supervisar este tipo de actividades. (Ej. un cambio en el proceso para permitir el acceso directo por una agencia gubernamental/gobierno). → Un cambio en el proceso para establecer vigilancia masiva. **6. Cambios legales significativos.** (Ej. cambios significativos –o propuestas de cambios– de leyes que dan a las autoridades gubernamentales más poder para hacer peticiones a los operadores). Ejemplo: → Cambios en las leyes de interceptación de comunicación.
PSI	El Portal de Servicio Interno "PSI" es una aplicación de consulta, permite que los integrantes de la Policía Nacional de Colombia, como clientes internos de la organización, encuentren en un sitio web toda la información para trámites internos, con altos niveles de seguridad.

CONCEPTO	EXPLICACIÓN
Solicitud	Una Petición es un requerimiento relacionado con la prestación de un servicio, en el ejercicio del deber de cooperación con las Autoridades Competentes. Una Petición puede contener una o varias solicitudes individualizadas, denominadas Solicitudes. Clases solicitudes: → Interceptaciones legales → Metadatos asociados a las comunicaciones: → Bloqueo y restricción de contenidos → Suspensiones geográficas o temporales de servicio
URL	Son las siglas en inglés de *Uniform Resource Locator* (en español, localizador uniforme de recursos), que sirve para nombrar recursos en internet. Esta denominación tiene un formato estándar y su propósito es asignar una dirección única a cada uno de los recursos disponibles en internet, como por ejemplo páginas, imágenes, vídeos, etc.


Telefónica